Evading IDS, Firewalls, and Honeypots

Module 12

Evading IDS, Firewalls, and Honeypots

Evading IDS and firewalls involves modifying attacks to escape detection by an organization's security systems, whereas honeypots are traps set to detect, deflect, or counteract unauthorized intrusion attempts.

Lab Scenario

ICON KEY

- 🗀 Valuable information
- ✎ Test your knowledge
- 💻 Web exercise
- 📖 Workbook review

The adoption of Internet use throughout the business world has boosted network usage in general. Organizations are using various network security measures such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), and "honeypots" to protect their networks, which are the preferred targets of hackers for compromising organizations' security. Attackers continue to find new ways to breach network security and attack these targets.

As an expert ethical hacker or pen tester, you must possess sound knowledge of the functions, role, placement, and design implementation of IDS, IPS, firewalls, and honeypots used in the organization, as well as understand the process that the attacker has used to evade the organization's security in order to detect their intrusion attempts.

The labs in this module give hands-on experience in auditing a network against IDS and firewall evasion attacks.

🗀 **Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots**

Lab Objectives

The objective of the lab is to evade the IDS and Firewall, and other tasks that include, but are not limited to:

- Detect intrusion attempts
- Detect malicious network traffic
- Detect intruders and their attack weapon
- Evade firewalls using various evasion techniques

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Windows 10 virtual machine
- Ubuntu virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 85 Minutes

Overview of Evading IDS, Firewalls, and Honeypots

IDSs, which provide an extra layer of security to the organization's infrastructure, are attractive targets for attackers. Attackers implement various IDS evasion techniques to bypass this security mechanism and compromise the infrastructure. Many IDS evasion techniques circumvent detect detection through multiple methods and can adapt to the best possible method for each system.

The firewall operates on a predefined set of rules. Using extensive knowledge and skill, an attacker can bypass the firewall by employing various bypassing techniques. Using these techniques, the attacker tricks the firewall to not filter the generated malicious traffic.

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to evade the IDS and firewall on the target network. Recommended labs that will assist you in learning various evasion techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Perform Intrusion Detection using Various Tools	√	√	√
	1.1 Detect Intrusions using Snort	√		√
	1.2 Detect Malicious Network Traffic using ZoneAlarm FREE FIREWALL 2019		√	√
	1.3 Detect Malicious Network Traffic using HoneyBOT	√		√
2	Evade Firewalls using Various Evasion Techniques	√	√	√
	2.1 Bypass Windows Firewall using Nmap Evasion Techniques	√		√
	2.2 Bypass Firewall Rules using HTTP/FTP Tunneling		√	√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv11 volume 1 book.

*****iLabs** - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Lab 1

Perform Intrusion Detection using Various Tools

An Intrusion Detection System (IDS) is a security software or hardware device used to monitor, detect, and protect networks or systems from malicious activities; it alerts security personnel immediately upon detecting intrusions.

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

Lab Scenario

The goal of the Intrusion Detection Analyst is to find possible attacks against a network. Recent years have witnessed a significant increase in Distributed Denial-of-Service (DDoS) attacks on the Internet, making network security a great concern. Analysts search for possible attacks by examining IDS logs and packet captures and corroborating them with firewall logs, known vulnerabilities, and general trending data from the Internet. IDS attacks are becoming more sophisticated; automatically reasoning the attack scenarios in real-time, and categorizing them has become a critical challenge. These processes result in huge amounts of data, which analysts must examine to detect a pattern. However, the overwhelming flow of events generated by IDS sensors make it difficult for security administrators to uncover hidden attack plans.

To become an expert penetration tester and security administrator, you must possess sound knowledge of network IPSs, IDSs, malicious network activity, and log information.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots

Lab Objectives

- Detect intrusions using Snort
- Detect malicious network traffic using ZoneAlarm FREE FIREWALL 2019
- Detect malicious network traffic using HoneyBOT

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine

- Windows Server 2016 virtual machine
- Windows Server 2019 virtual machine
- Ubuntu virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- Snort located at **E:\CEH-Tools\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort**
- ZoneAlarm FREE FIREWALL 2019 located at **E:\CEH-Tools\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots\Firewalls\ZoneAlarm FREE FIREWALL 2019**
- HoneyBOT located at **E:\CEH-Tools\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots\Honeypot Tools\HoneyBOT**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest version, the screenshots shown in the lab might differ.

Lab Duration

Time: 55 Minutes

Overview of Intrusion Detection Systems

Intrusion detection systems are highly useful as they monitor both the inbound and outbound traffic of the network and continuously inspects the data for suspicious activities that may indicate a network or system security breach. The IDS checks traffic for signatures that match known intrusion patterns and signals an alarm when a match is detected. It can be categorized into active and passive, depending on its functionality: an IDS is generally passive and is used to detect intrusions, while an intrusion prevention system (IPS) is considered as an active IDS, as it is not only used to detect the intrusion on the network, but also prevent them.

Main Functions of IDS:

- Gathers and analyzes information from within a computer or a network, to identify the possible violations of security policy
- Also referred to as a "packet-sniffer," which intercepts packets traveling along various communication mediums and protocols
- Evaluates traffic for suspected intrusions and signals an alarm after detection

Lab Tasks

TASK 1

Detect Intrusions using Snort

Here, we will use Snort to detect network intrusions.

1. Turn on the **Windows 10** and **Windows Server 2019** virtual machines.

TASK 1.1

Install Snort

2. In the **Windows Server 2019** virtual machine, log in with the credentials **Administrator** and **Pa$$w0rd**.

3. Navigate to **Z:\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort** and double-click the **Snort_2_9_15_Installer.exe** file to start the Snort installation.

Snort is an open-source network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks.

Note: If an **Open File - Security warning** pop-up window appears, click **Run**.

4. Accept the **License Agreement** and install Snort by selecting the default options that appear **step by step** in the wizard.

5. A window appears after the successful installation of Snort; click **Close**.

6. Click **OK** to exit the **Snort Installation** window.

Note: Snort requires **WinPcap** to be installed on your machine. In this lab environment, we have already installed WinPcap drivers for packet capturing.

It can perform protocol analysis and content searching/matching and is used to detect a variety of attacks and probes such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and OS fingerprinting attempts.

7. By default, Snort installs itself in **C:\Snort** (C:\ or D:\, depending on the disk drive in which the OS is installed).

8. Navigate to the **etc** folder in the specified location, **Z:\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules-snapshot-29150\etc** of the Snort rules; copy **snort.conf** and paste it in **C:\Snort\etc**.

9. **snort.conf** is already present in **C:\Snort\etc**; replace the file with the newly copied file.

Snort uses a flexible rules language to describe traffic to collect or pass, as well as a detection engine that utilizes a modular plug-in architecture.

10. Copy the **so_rules** folder from **Z:\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules-snapshot-29150** and paste into **C:\Snort**.

11. Copy the **preproc_rules** folder from **Z:\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules-snapshot-29150**, and paste it into **C:\Snort**. The **preproc_rules** folder is already present in **C:\Snort**; replace this folder with the **preproc_rules** folder taken from the specified location.

12. Using the same method, copy the **rules** folder from **Z:\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules-snapshot-29150** and paste into **C:\Snort**.

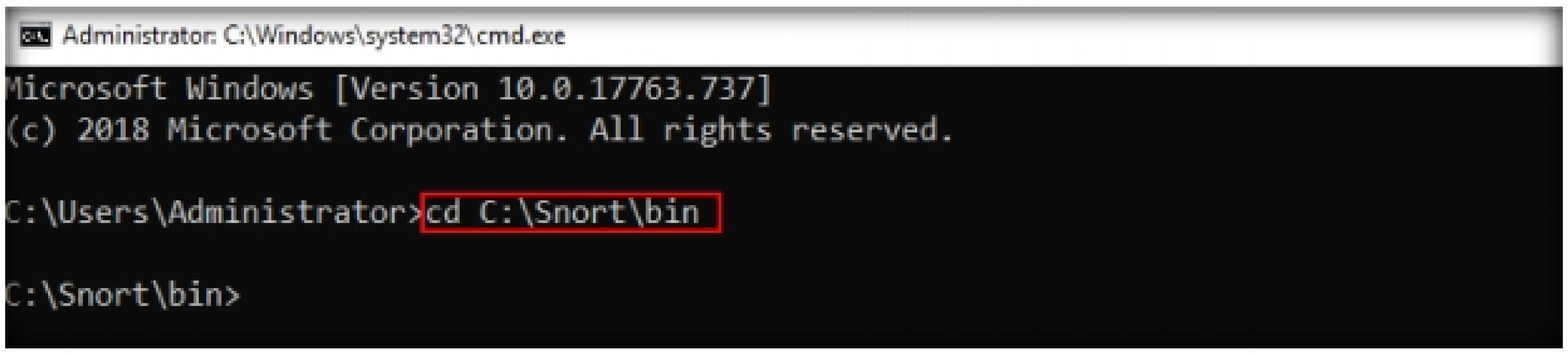
13. Now right-click on the **Windows Start** icon and click **Run** from the menu.

TASK 1.2

Verify Snort Alert

14. The **Run** window appears; type **cmd** in the **Open** field and click **OK** to launch command prompt window.

15. The **Command Prompt** window appears; type **cd C:\Snort\bin** and press **Enter** to access the bin folder in the command prompt.



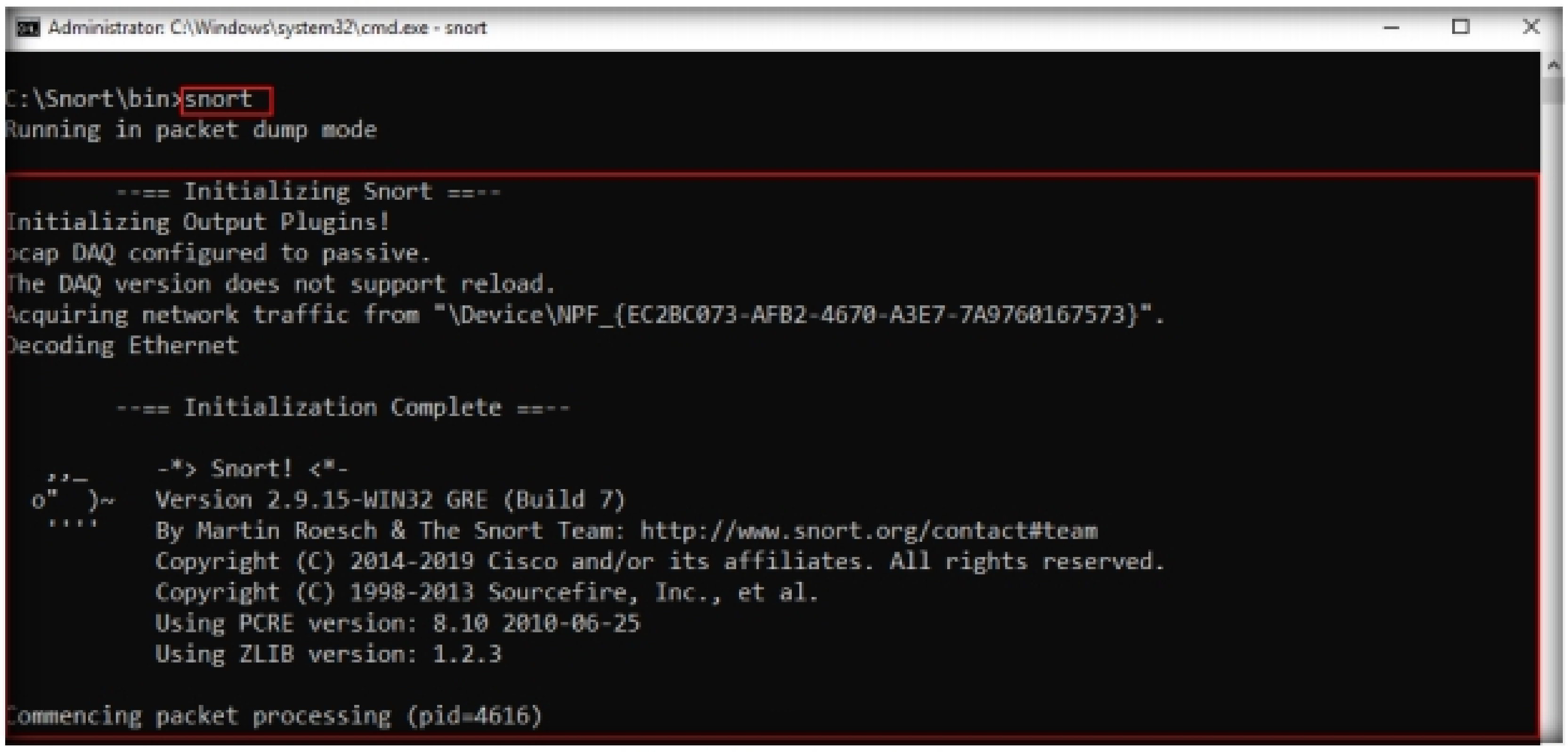
```
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd C:\Snort\bin

C:\Snort\bin>
```

Figure 1.1.1: Accessing Snort Directory in Command Prompt

Uses of Snort:

- Straight packet sniffer such as tcpdump
- Packet logger (useful for network traffic debugging, etc.)
- Network intrusion prevention system.

16. Type **snort** and press **Enter**.

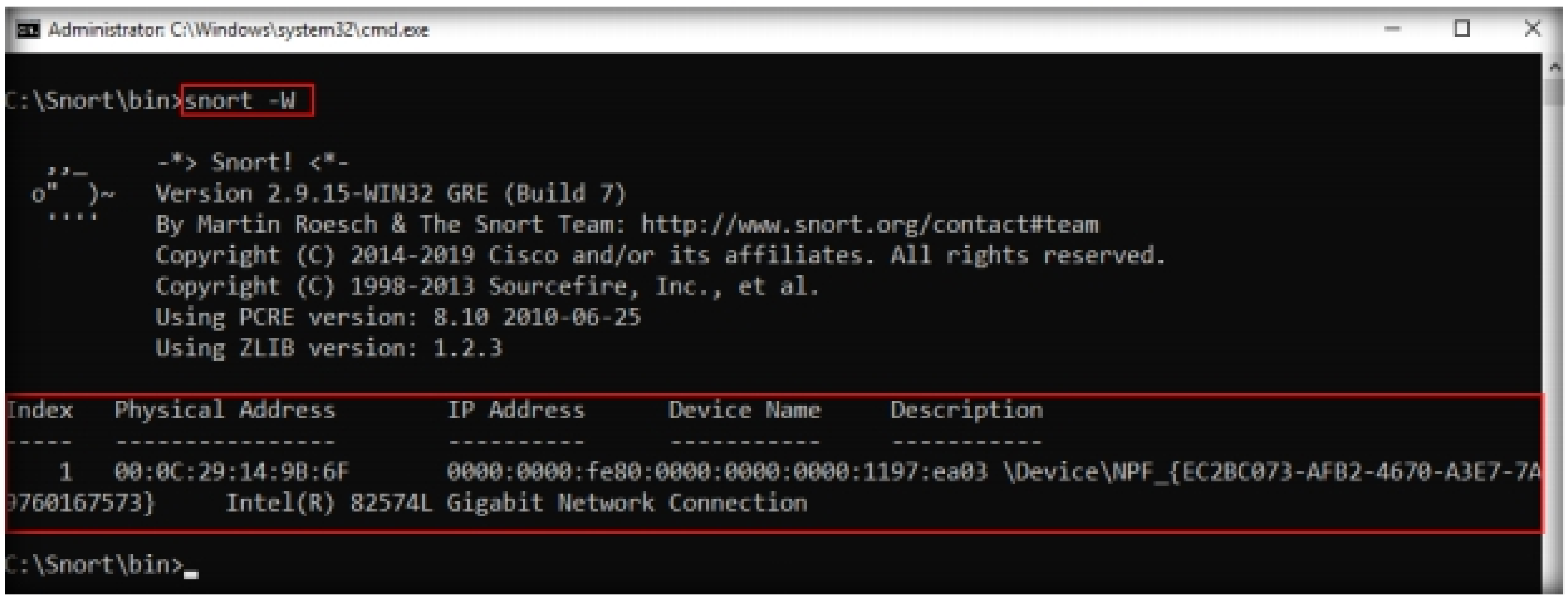


```
C:\Snort\bin>snort
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{EC2BC073-AFB2-4670-A3E7-7A9760167573}".
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.15-WIN32 GRE (Build 7)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.3

Commencing packet processing (pid=4616)
```

Figure 1.1.2: Verifying Snort

17. Snort initializes; wait for it to complete. After completion press **Ctrl+C**, Snort exits and comes back to **C:\Snort\bin**.

18. Now type **snort -W**. This command lists your machine's physical address, IP address, and Ethernet Drivers, but all are disabled by default.



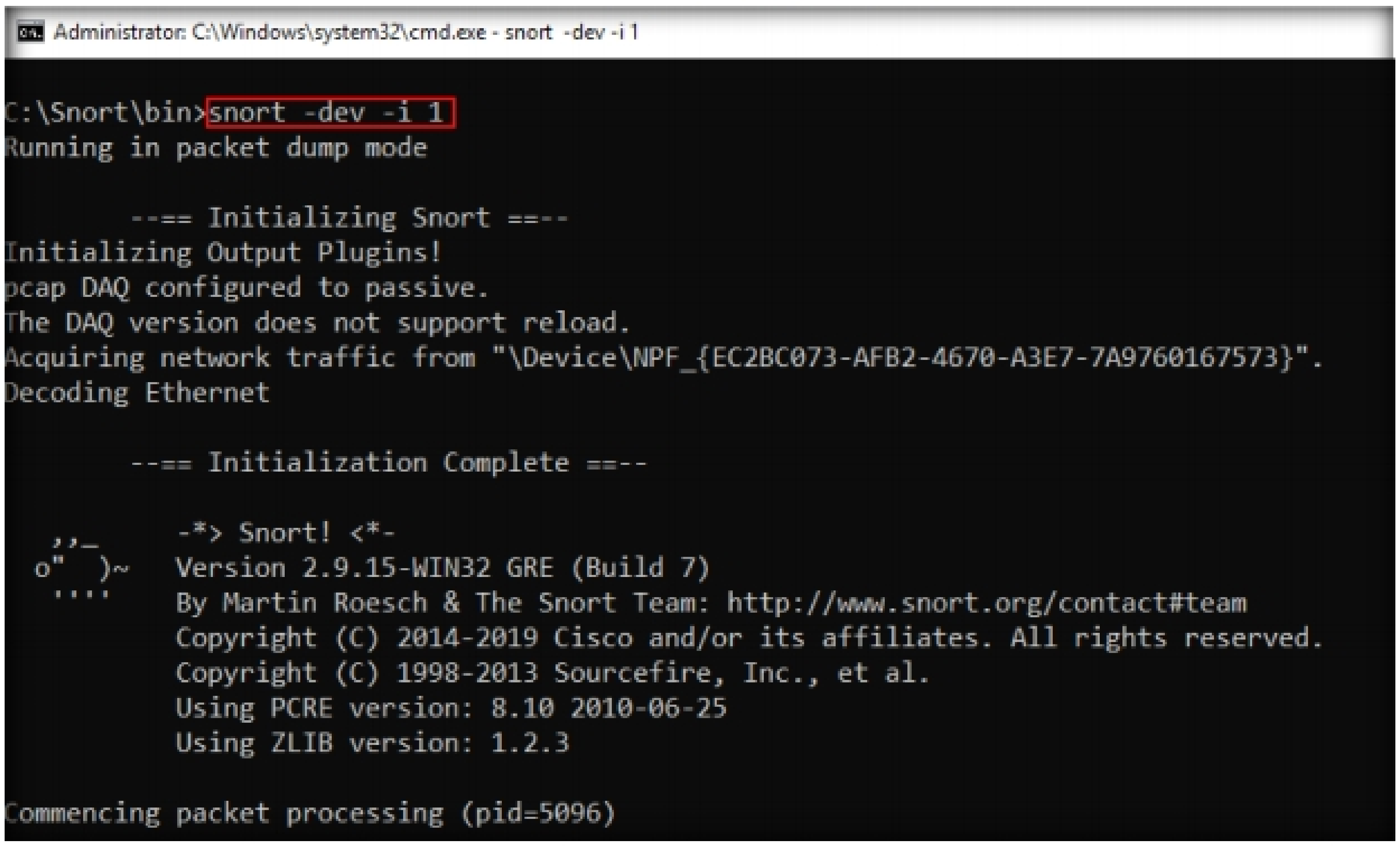
```
C:\Snort\bin>snort -W

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.15-WIN32 GRE (Build 7)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.3

Index   Physical Address        IP Address      Device Name     Description
-----   ----------------        ----------      -----------     -----------
    1   00:0C:29:14:9B:6F       0000:0000:fe80:0000:0000:0000:1197:ea03 \Device\NPF_{EC2BC073-AFB2-4670-A3E7-7A
9760167573}     Intel(R) 82574L Gigabit Network Connection

C:\Snort\bin>_
```

Figure 1.1.3: Finding out the physical address

19. Observe your Ethernet Driver **index number** and write it down (in this lab, it is **1**).

20. To enable the Ethernet Driver, in the command prompt, type **snort -dev -i 1** and press **Enter**.

21. You see a rapid scroll text in the command prompt, which means that the Ethernet Driver is enabled and working properly.

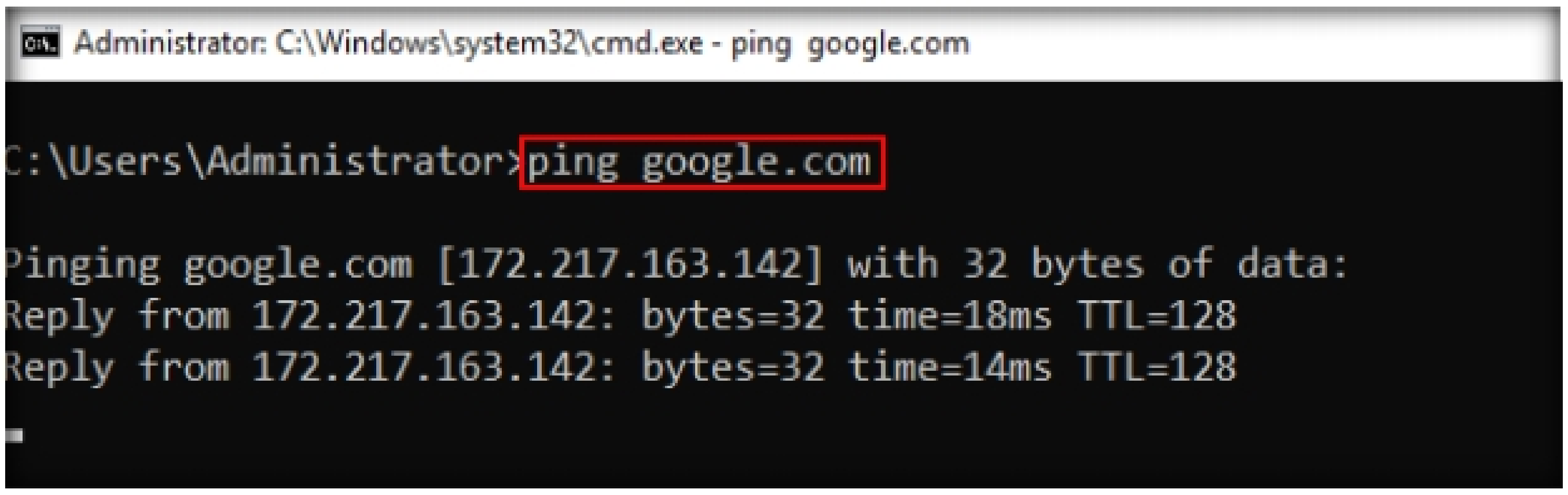

Administrator: C:\Windows\system32\cmd.exe - snort -dev -i 1

```
C:\Snort\bin>snort -dev -i 1
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{EC2BC073-AFB2-4670-A3E7-7A9760167573}".
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.15-WIN32 GRE (Build 7)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.3

Commencing packet processing (pid=5096)
```

Figure 1.1.4: Enabling Ethernet driver

22. Leave the Snort command prompt window open, and launch another command prompt window.

23. In a new command prompt, type **ping google.com** and press **Enter**.

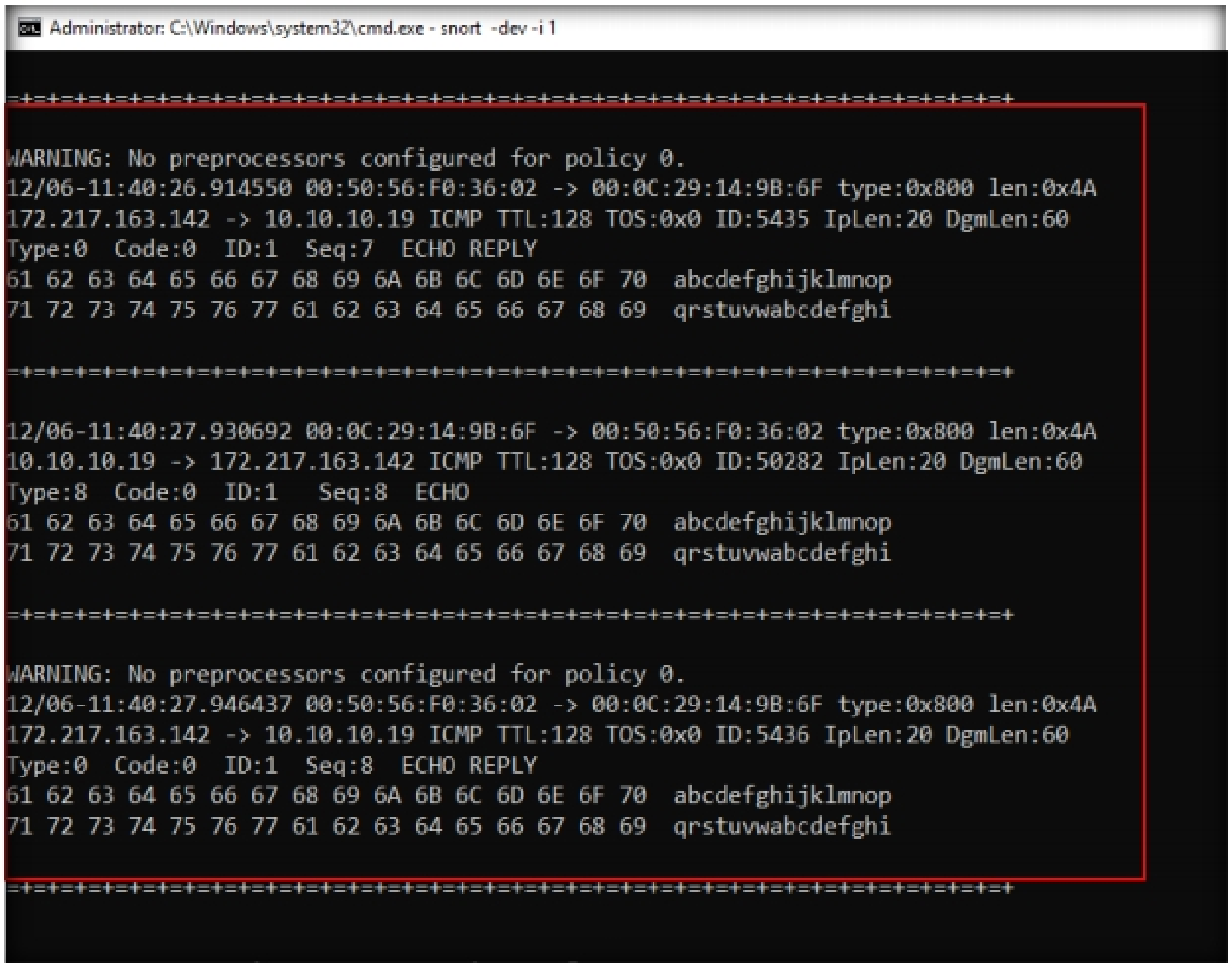

Administrator: C:\Windows\system32\cmd.exe - ping google.com

```
C:\Users\Administrator>ping google.com

Pinging google.com [172.217.163.142] with 32 bytes of data:
Reply from 172.217.163.142: bytes=32 time=18ms TTL=128
Reply from 172.217.163.142: bytes=32 time=14ms TTL=128
```

Figure 1.1.5: Ping google.com command

24. This ping command triggers a Snort alert in the Snort command prompt with rapid scrolling text.

Note: The Google IP address will differ in your lab environment.


Administrator: C:\Windows\system32\cmd.exe - snort -dev -i 1

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
12/06-11:40:26.914550 00:50:56:F0:36:02 -> 00:0C:29:14:9B:6F type:0x800 len:0x4A
172.217.163.142 -> 10.10.10.19 ICMP TTL:128 TOS:0x0 ID:5435 IpLen:20 DgmLen:60
Type:0  Code:0  ID:1  Seq:7  ECHO REPLY
61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70  abcdefghijklmnop
71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69  qrstuvwabcdefghi

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

12/06-11:40:27.930692 00:0C:29:14:9B:6F -> 00:50:56:F0:36:02 type:0x800 len:0x4A
10.10.10.19 -> 172.217.163.142 ICMP TTL:128 TOS:0x0 ID:50282 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:8  ECHO
61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70  abcdefghijklmnop
71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69  qrstuvwabcdefghi

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
12/06-11:40:27.946437 00:50:56:F0:36:02 -> 00:0C:29:14:9B:6F type:0x800 len:0x4A
172.217.163.142 -> 10.10.10.19 ICMP TTL:128 TOS:0x0 ID:5436 IpLen:20 DgmLen:60
Type:0  Code:0  ID:1  Seq:8  ECHO REPLY
61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70  abcdefghijklmnop
71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69  qrstuvwabcdefghi

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Figure 1.1.6: Snort showing captured Google request

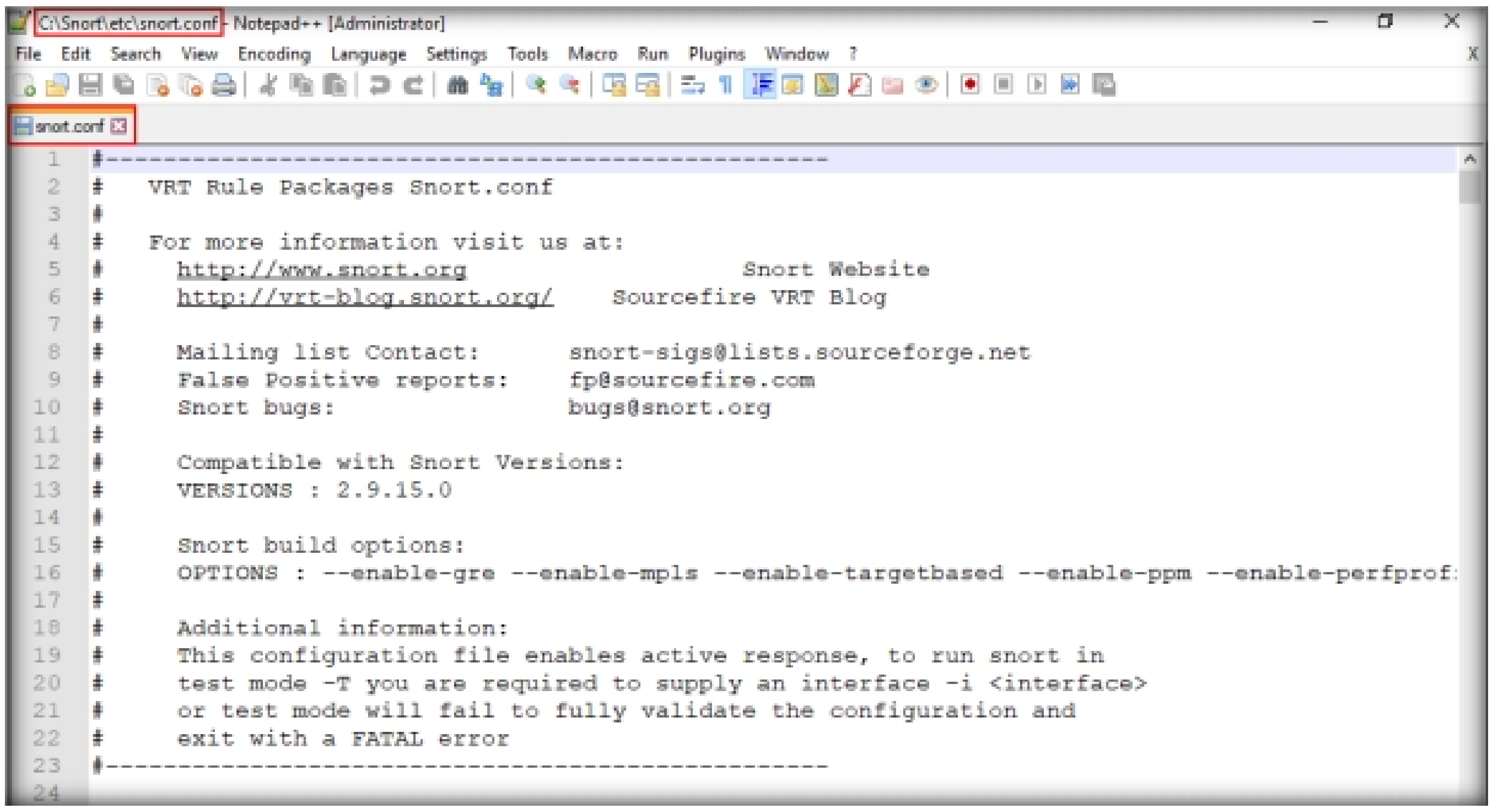
25. Close both command prompt windows. The verification of Snort installation and the triggering alert is complete, and Snort is working correctly in verbose mode.

TASK 1.3

Configure snort.conf File

26. Configure the **snort.conf** file, located at **C:\Snort\etc**.

27. Open the **snort.conf** file with **Notepad++**.



```
#--------------------------------------------------
#   VRT Rule Packages Snort.conf
#
#   For more information visit us at:
#     http://www.snort.org                   Snort Website
#     http://vrt-blog.snort.org/    Sourcefire VRT Blog
#
#     Mailing list Contact:      snort-sigs@lists.sourceforge.net
#     False Positive reports:    fp@sourcefire.com
#     Snort bugs:                bugs@snort.org
#
#     Compatible with Snort Versions:
#     VERSIONS : 2.9.15.0
#
#     Snort build options:
#     OPTIONS : --enable-gre --enable-mpls --enable-targetbased --enable-ppm --enable-perfprof:
#
#     Additional information:
#     This configuration file enables active response, to run snort in
#     test mode -T you are required to supply an interface -i <interface>
#     or test mode will fail to fully validate the configuration and
#     exit with a FATAL error
#--------------------------------------------------
```

Figure 1.1.7: Snort.conf file in Notepad++

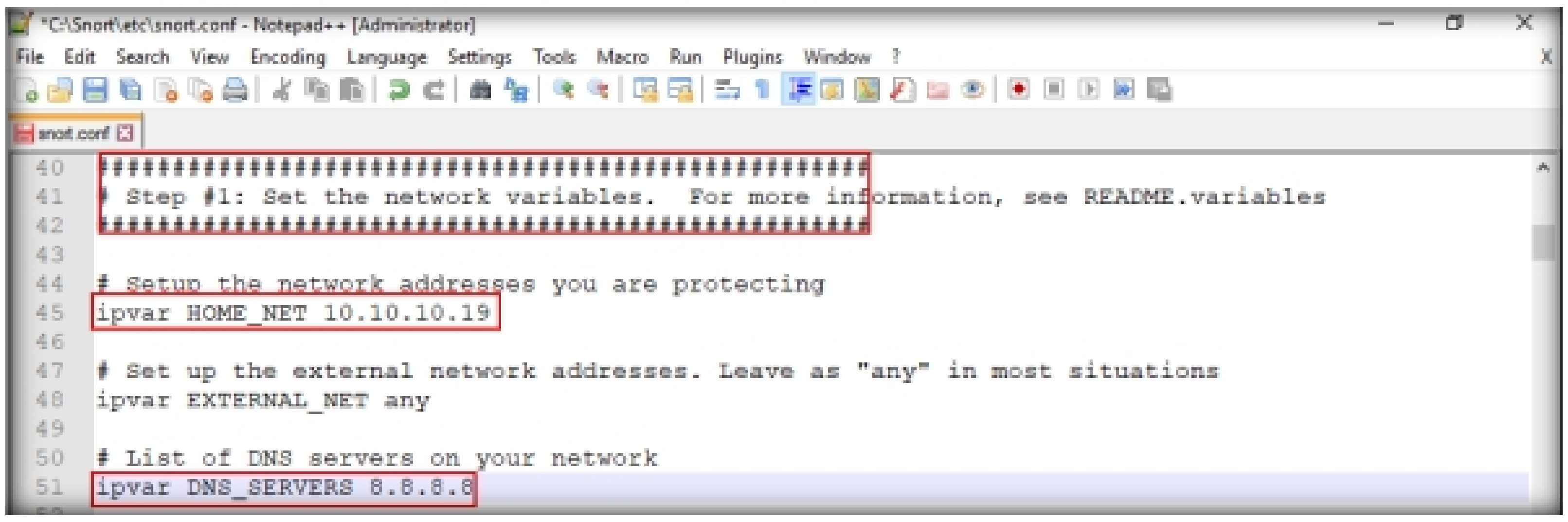
28. Scroll down to the **Step #1: Set the network variables** section (Line 41) of the **snort.conf** file. In the **HOME_NET** line (Line 45), replace **any** with the IP addresses of the machine (target machine) on which Snort is running. Here, the target machine is **Windows Server 2019** and the IP address is **10.10.10.19**.

Note: This IP address may vary in your lab environment.

29. Leave the **EXTERNAL_NET any** line as it is.

30. If you have a **DNS Server**, then make changes in the **DNS_SERVERS** line by replacing **$HOME_NET** with your DNS Server IP address; otherwise, leave this line as it is.

Note: Here, the DNS server is **8.8.8.8**.


*C:\Snort\etc\snort.conf - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
snort.conf

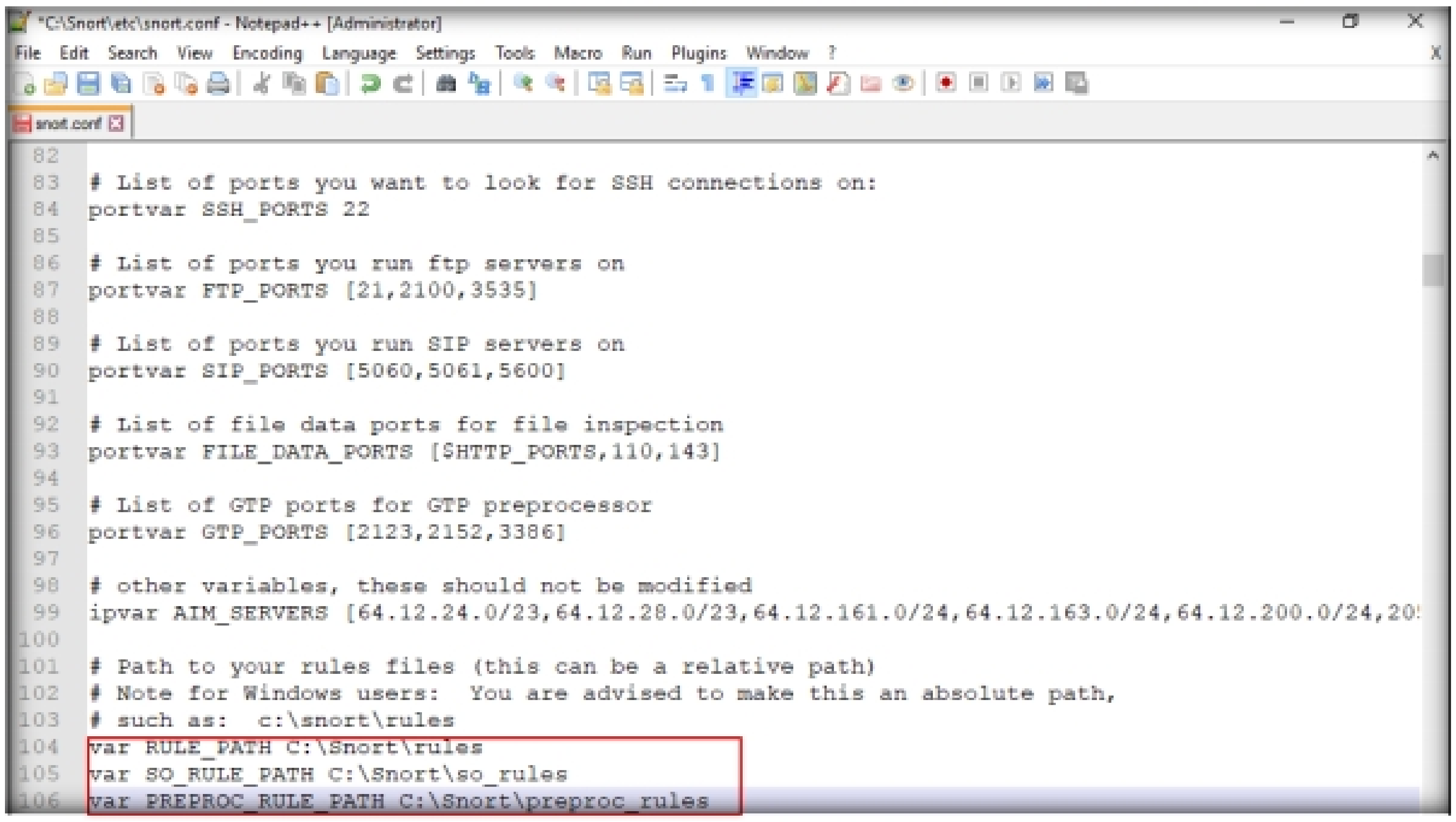
```
40 ###################################################
41 # Step #1: Set the network variables.  For more information, see README.variables
42 ###################################################
43
44 # Setup the network addresses you are protecting
45 ipvar HOME_NET 10.10.10.19
46
47 # Set up the external network addresses. Leave as "any" in most situations
48 ipvar EXTERNAL_NET any
49
50 # List of DNS servers on your network
51 ipvar DNS_SERVERS 8.8.8.8
```

Figure 1.1.8: Set the network variables

31. The same applies to SMTP_SERVERS, HTTP_SERVERS, SQL_SERVERS, TELNET_SERVERS, and SSH_SERVERS.

32. Remember that if you do not have any servers running on your machine, leave the line as it is. **DO NOT** make any changes in that line.

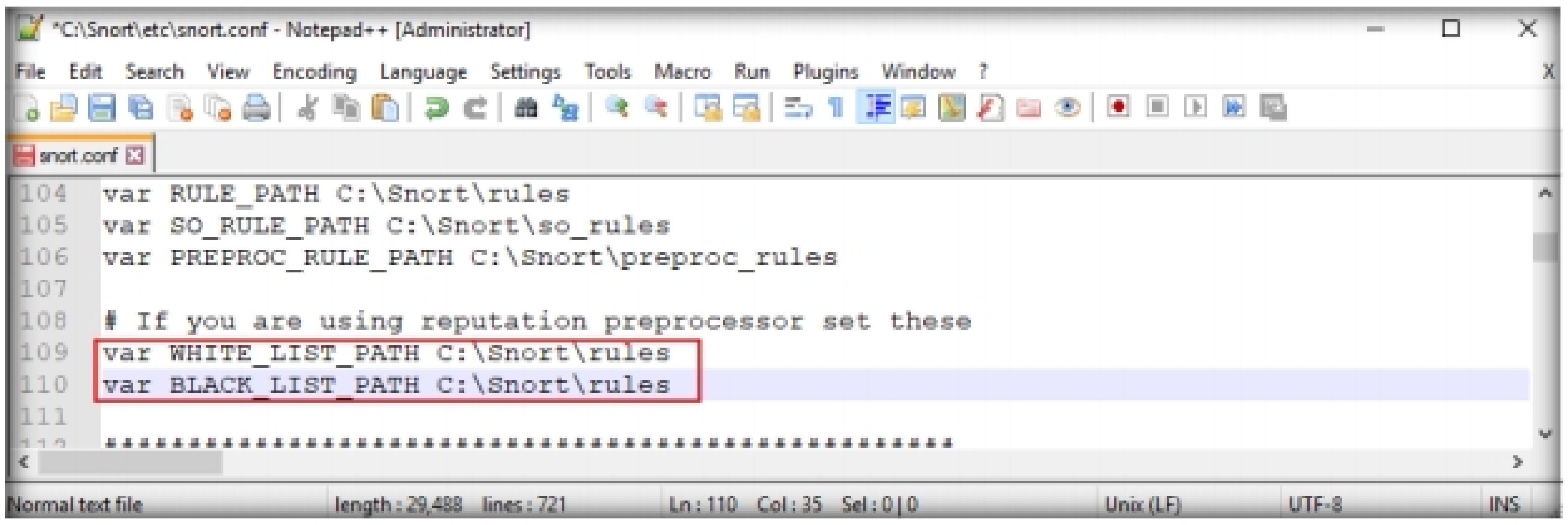
33. Scroll down to **RULE_PATH** (Line 104). In Line 104, replace **../rules** with **C:\Snort\rules**; in Line 105, replace **../so_rules** with **C:\Snort\so_rules**; and in Line 106, replace **../preproc_rules** with **C:\Snort\preproc_rules**.


*C:\Snort\etc\snort.conf - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
snort.conf

```
 82
 83 # List of ports you want to look for SSH connections on:
 84 portvar SSH_PORTS 22
 85
 86 # List of ports you run ftp servers on
 87 portvar FTP_PORTS [21,2100,3535]
 88
 89 # List of ports you run SIP servers on
 90 portvar SIP_PORTS [5060,5061,5600]
 91
 92 # List of file data ports for file inspection
 93 portvar FILE_DATA_PORTS [$HTTP_PORTS,110,143]
 94
 95 # List of GTP ports for GTP preprocessor
 96 portvar GTP_PORTS [2123,2152,3386]
 97
 98 # other variables, these should not be modified
 99 ipvar AIM_SERVERS [64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24,64.12.200.0/24,20
100
101 # Path to your rules files (this can be a relative path)
102 # Note for Windows users:  You are advised to make this an absolute path,
103 # such as:  c:\snort\rules
104 var RULE_PATH C:\Snort\rules
105 var SO_RULE_PATH C:\Snort\so_rules
106 var PREPROC_RULE_PATH C:\Snort\preproc_rules
```

Figure 1.1.9: Snort Rules Path

34. In Lines 109 and 110, replace **../rules** with **C:\Snort\rules**. Minimize the **Notepad++** window.


*C:\Snort\etc\snort.conf - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
snort.conf
Normal text file
length : 29,488 lines : 721
Ln : 110 Col : 35 Sel : 0 | 0
Unix (LF)
UTF-8
INS

```
104  var RULE_PATH C:\Snort\rules
105  var SO_RULE_PATH C:\Snort\so_rules
106  var PREPROC_RULE_PATH C:\Snort\preproc_rules
107
108  # If you are using reputation preprocessor set these
109  var WHITE_LIST_PATH C:\Snort\rules
110  var BLACK_LIST_PATH C:\Snort\rules
111
```

Figure 1.1.10: Snort Rules Path

35. Navigate to **C:\Snort\rules**, and create two text files; name them **white_list** and **black_list** and change their file extensions from **.txt** to **.rules**.

Note: To create a text file, right-click anywhere inside the **rules** window and navigate to **New** → **Text Document**.

36. While changing the extension, if any pop-up appears, click **Yes**.

37. Switch back to **Notepad ++**, scroll down to the **Step #4: Configure dynamic loaded libraries** section (Line 238). **Configure dynamic loaded libraries** in this section.

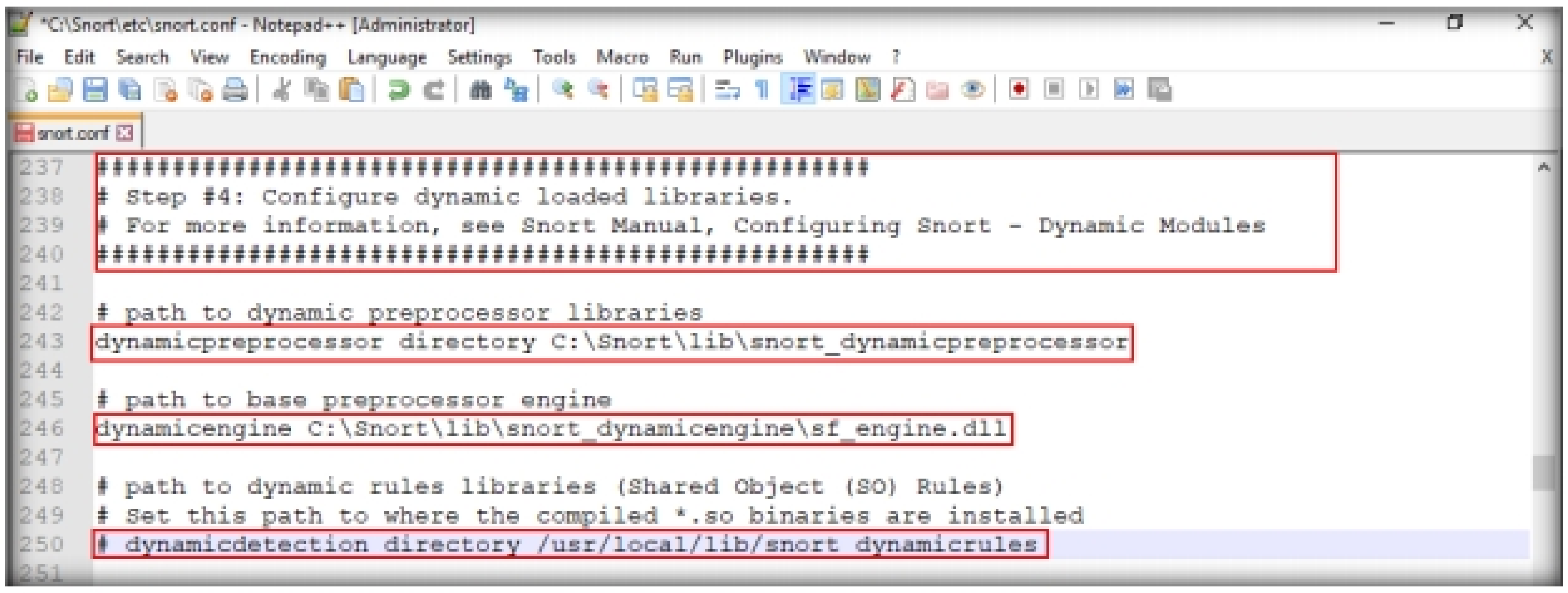
38. Add the path to dynamic preprocessor libraries (Line 243); replace **/usr/local/lib/snort_dynamicpreprocessor/** with your dynamic preprocessor libraries folder location.

39. In this lab, the dynamic preprocessor libraries are located at **C:\Snort\lib\snort_dynamicpreprocessor**.

40. At the path to base preprocessor (or dynamic) engine (Line 246), replace **/usr/local/lib/snort_dynamicengine/libsf_engine.so** with your base preprocessor engine **C:\Snort\lib\snort_dynamicengine\sf_engine.dll**.

41. Ensure that the dynamic rules libraries (Line 250) is commented out, as you have already configured the libraries in dynamic preprocessor libraries.

Note: Add **<space>** in between **#** and **dynamicdetection** (Line 250).


*C:\Snort\etc\snort.conf - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
snort.conf

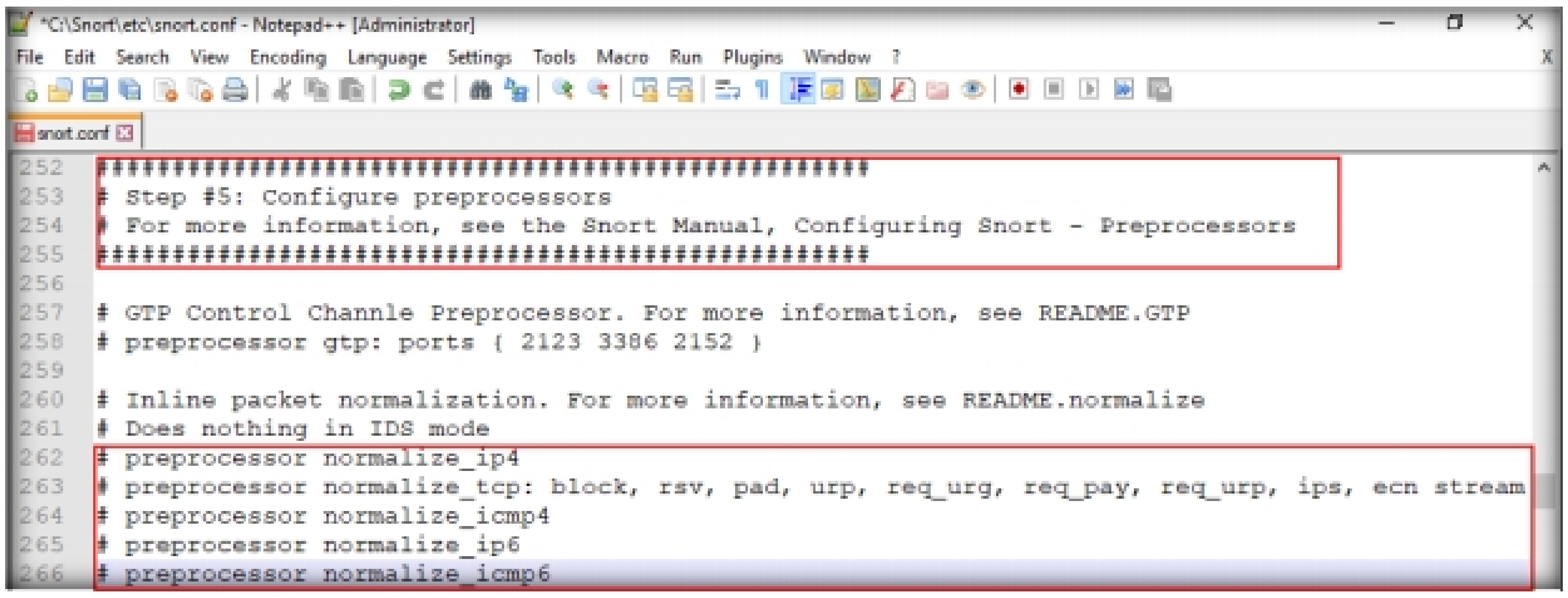
```
237  ###################################################
238  # Step #4: Configure dynamic loaded libraries.
239  # For more information, see Snort Manual, Configuring Snort - Dynamic Modules
240  ###################################################
241
242  # path to dynamic preprocessor libraries
243  dynamicpreprocessor directory C:\Snort\lib\snort_dynamicpreprocessor
244
245  # path to base preprocessor engine
246  dynamicengine C:\Snort\lib\snort_dynamicengine\sf_engine.dll
247
248  # path to dynamic rules libraries (Shared Object (SO) Rules)
249  # Set this path to where the compiled *.so binaries are installed
250  # dynamicdetection directory /usr/local/lib/snort_dynamicrules
```

Figure 1.1.11: Configuring Dynamic Loaded Libraries

42. Scroll down to the **Step #5: Configure preprocessors** section (Line 253), the listed preprocessor. This does nothing in IDS mode, however, it generates errors at runtime.

43. Comment out all the preprocessors listed in this section by adding **'#'** and **<space>** before each preprocessor rule (262-266).

Note: To 'comment out' is to render a block of code inert by turning it into a comment.

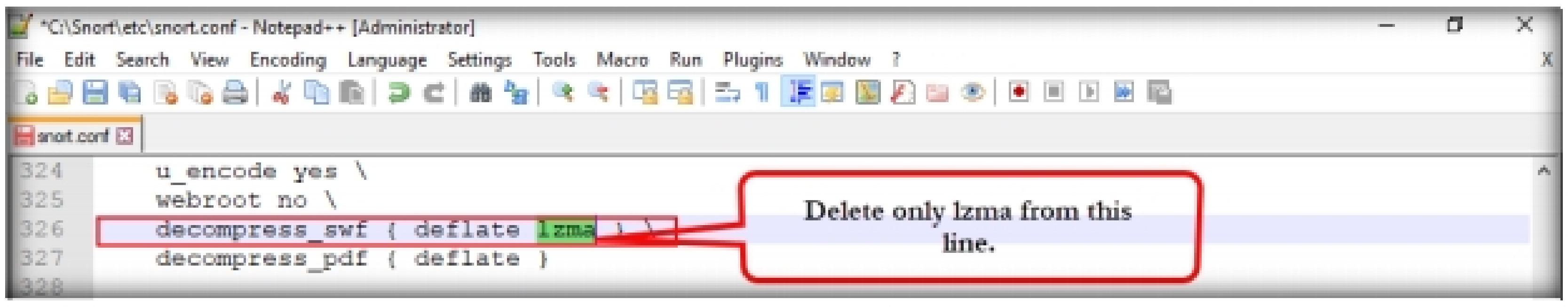


*C:\Snort\etc\snort.conf - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
snort.conf

```
252 ###################################################
253 # Step #5: Configure preprocessors
254 # For more information, see the Snort Manual, Configuring Snort - Preprocessors
255 ###################################################
256
257 # GTP Control Channle Preprocessor. For more information, see README.GTP
258 # preprocessor gtp: ports { 2123 3386 2152 }
259
260 # Inline packet normalization. For more information, see README.normalize
261 # Does nothing in IDS mode
262 # preprocessor normalize_ip4
263 # preprocessor normalize_tcp: block, rsv, pad, urp, req_urg, req_pay, req_urp, ips, ecn stream
264 # preprocessor normalize_icmp4
265 # preprocessor normalize_ip6
266 # preprocessor normalize_icmp6
```

Figure 1.1.12: Configuring Preprocessors

44. Scroll down to line 326 and delete **lzma** keyword and a **<space>**.



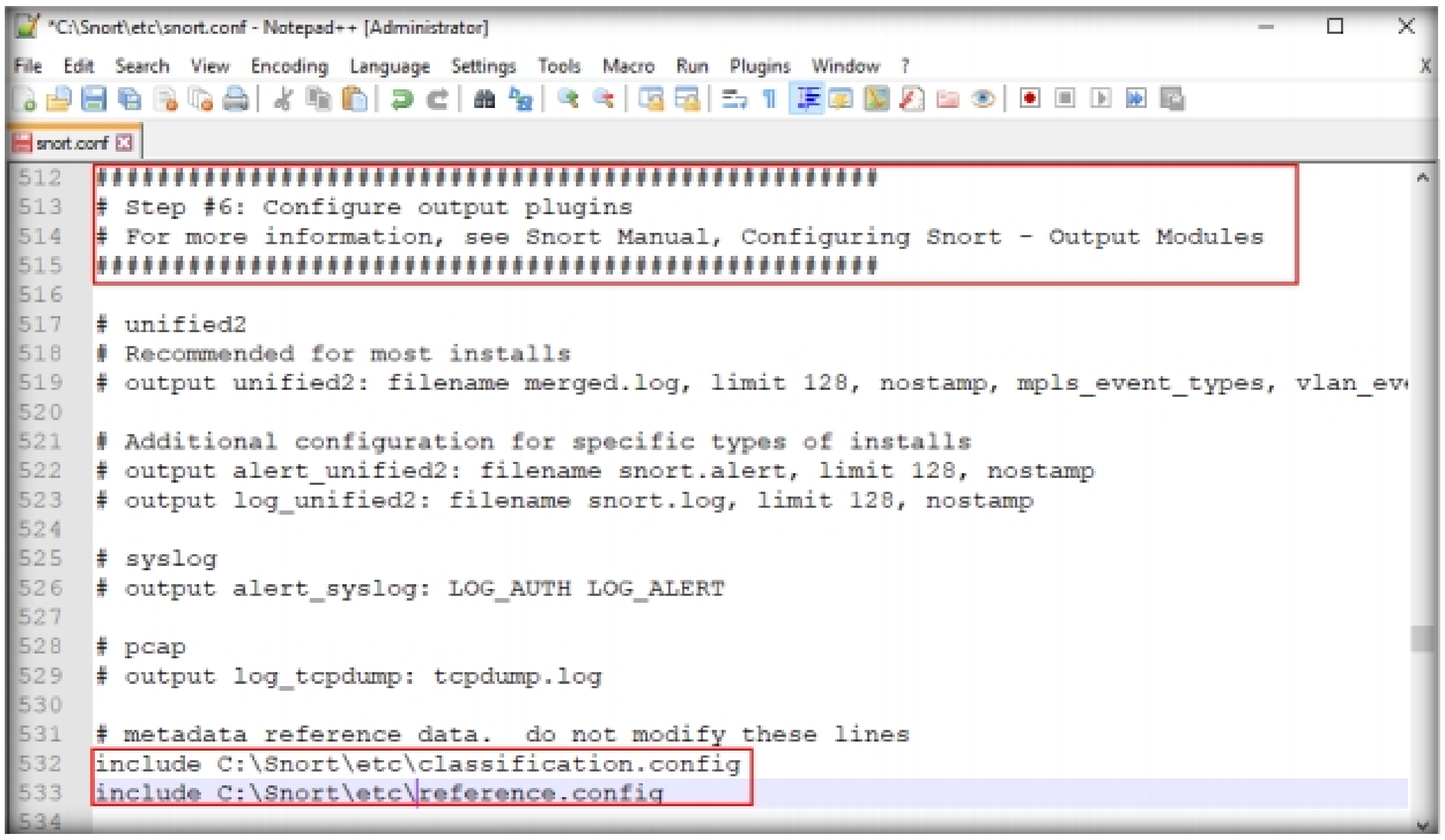
*C:\Snort\etc\snort.conf - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
snort.conf
Delete only lzma from this line.

```
324     u_encode yes \
325     webroot no \
326     decompress_swf { deflate lzma } \
327     decompress_pdf { deflate }
328
```

Figure 1.1.13: Deleting lzma

45. Scroll down to **Step #6: Configure output plugins** (Line 513). In this step, provide the location of the **classification.config** and **reference.config** files.

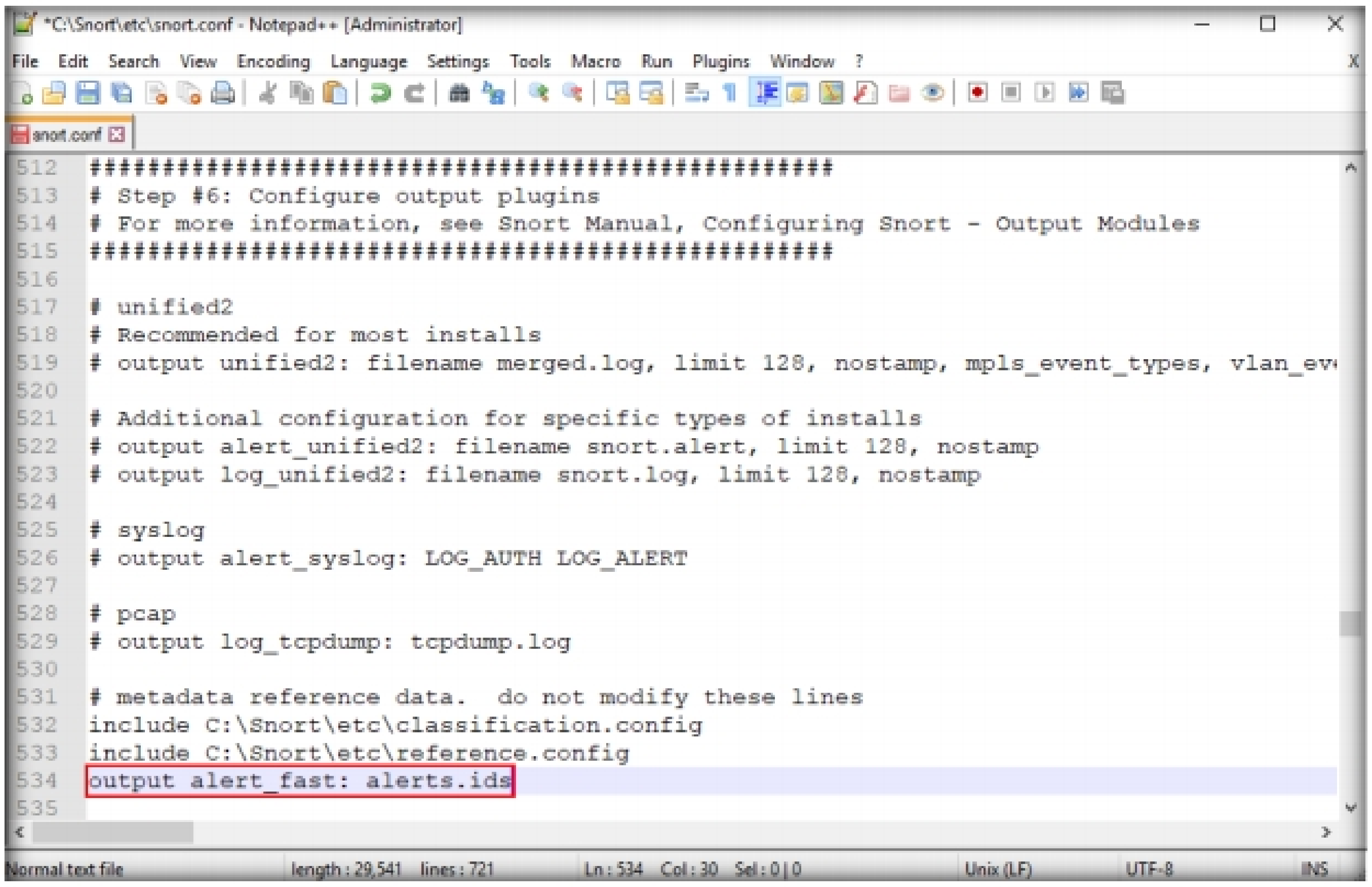
46. These two files are in **C:\Snort\etc**. Provide this location of files in the configure output plugins (in Lines 532 and 533) (i.e., **C:\Snort\etc\classification.config** and **C:\Snort\etc\reference.config**).


*C:\Snort\etc\snort.conf - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
snort.conf

```
512 ###################################################
513 # Step #6: Configure output plugins
514 # For more information, see Snort Manual, Configuring Snort - Output Modules
515 ###################################################
516 
517 # unified2
518 # Recommended for most installs
519 # output unified2: filename merged.log, limit 128, nostamp, mpls_event_types, vlan_ev
520 
521 # Additional configuration for specific types of installs
522 # output alert_unified2: filename snort.alert, limit 128, nostamp
523 # output log_unified2: filename snort.log, limit 128, nostamp
524 
525 # syslog
526 # output alert_syslog: LOG_AUTH LOG_ALERT
527 
528 # pcap
529 # output log_tcpdump: tcpdump.log
530 
531 # metadata reference data.  do not modify these lines
532 include C:\Snort\etc\classification.config
533 include C:\Snort\etc\reference.config
534 
```

Figure 1.1.14: Configuring output plugins

47. In **Step #6**, add to line (534) **output alert_fast: alerts.ids**: this command orders Snort to dump all logs into the **alerts.ids** file.


*C:\Snort\etc\snort.conf - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
snort.conf
Normal text file
length : 29,541 lines : 721
Ln : 534 Col : 30 Sel : 0 | 0
Unix (LF)
UTF-8
INS

```
512 ###################################################
513 # Step #6: Configure output plugins
514 # For more information, see Snort Manual, Configuring Snort - Output Modules
515 ###################################################
516 
517 # unified2
518 # Recommended for most installs
519 # output unified2: filename merged.log, limit 128, nostamp, mpls_event_types, vlan_ev
520 
521 # Additional configuration for specific types of installs
522 # output alert_unified2: filename snort.alert, limit 128, nostamp
523 # output log_unified2: filename snort.log, limit 128, nostamp
524 
525 # syslog
526 # output alert_syslog: LOG_AUTH LOG_ALERT
527 
528 # pcap
529 # output log_tcpdump: tcpdump.log
530 
531 # metadata reference data.  do not modify these lines
532 include C:\Snort\etc\classification.config
533 include C:\Snort\etc\reference.config
534 output alert_fast: alerts.ids
535 
```

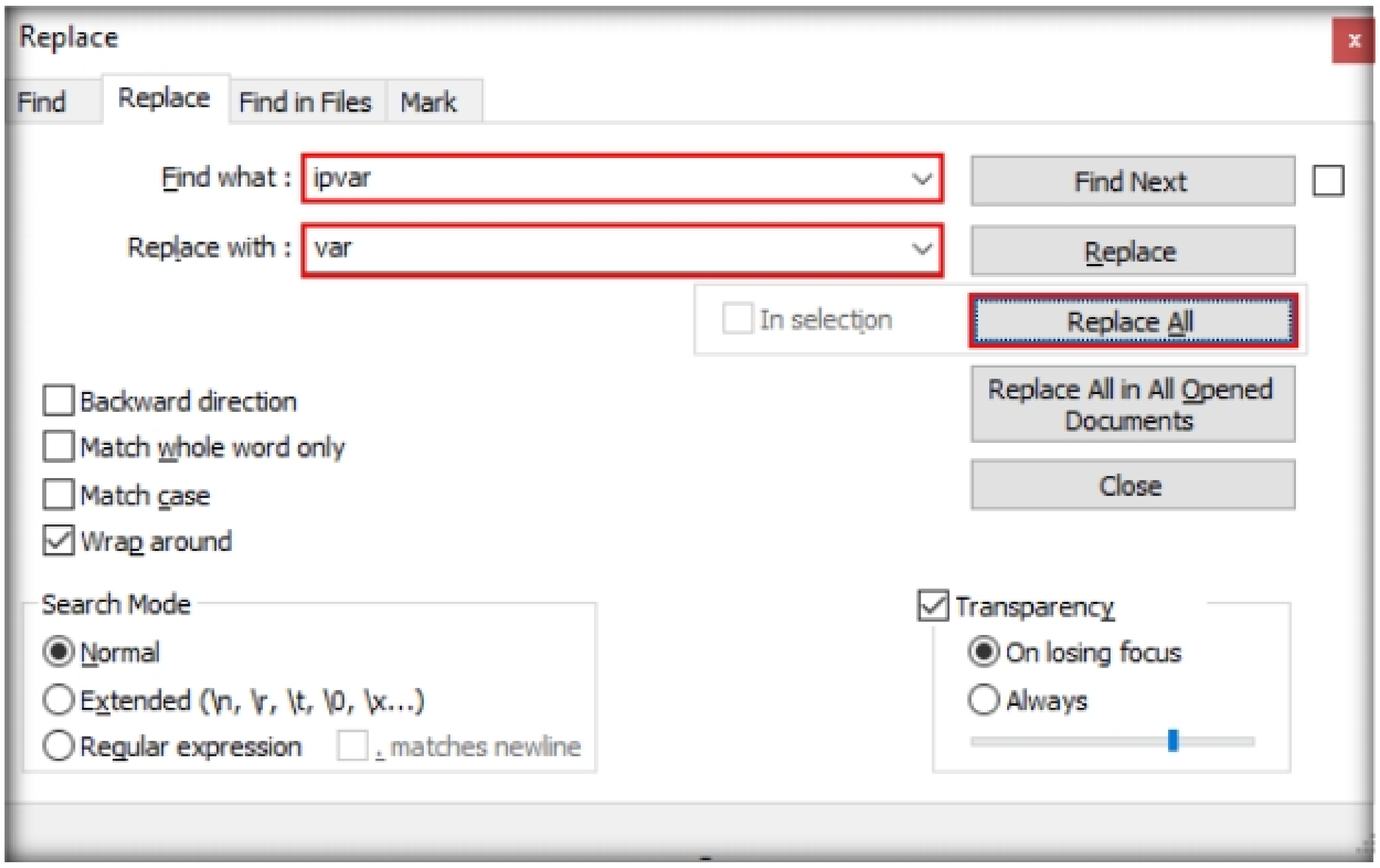
Figure 1.1.15: Adding output alert

48. In the **snort.conf** file, find and replace the **ipvar** string with **var**. To do this, press **Ctrl+H** on the keyboard. The **Replace** window appears; enter **ipvar** in the **Find what :** text field, enter **var** in the **Replace with :** text field, and click **Replace All**.

Note: You will get a notification saying 11 occurrences were replaced.

49. By default, the string is **ipvar**, which is not recognized by Snort: replace with the **var** string, and then **close** the window.

Note: Snort now supports multiple configurations based on VLAN Id or IP subnet within a single instance of Snort. This allows administrators to specify multiple snort configuration files and bind each configuration to one or more VLANs or subnets rather than running one Snort for each configuration required.



Find what : ipvar

Replace with : var

☐ In selection

☐ Backward direction

☐ Match whole word only

☐ Match case

☑ Wrap around

● Normal

○ Extended (\n, \r, \t, \0, \x...)

○ Regular expression ☐ . matches newline

☑ Transparency

● On losing focus

○ Always

Figure 1.1.16: Replacing ipvar with var

50. Click **Close** to close the **Replace** window.

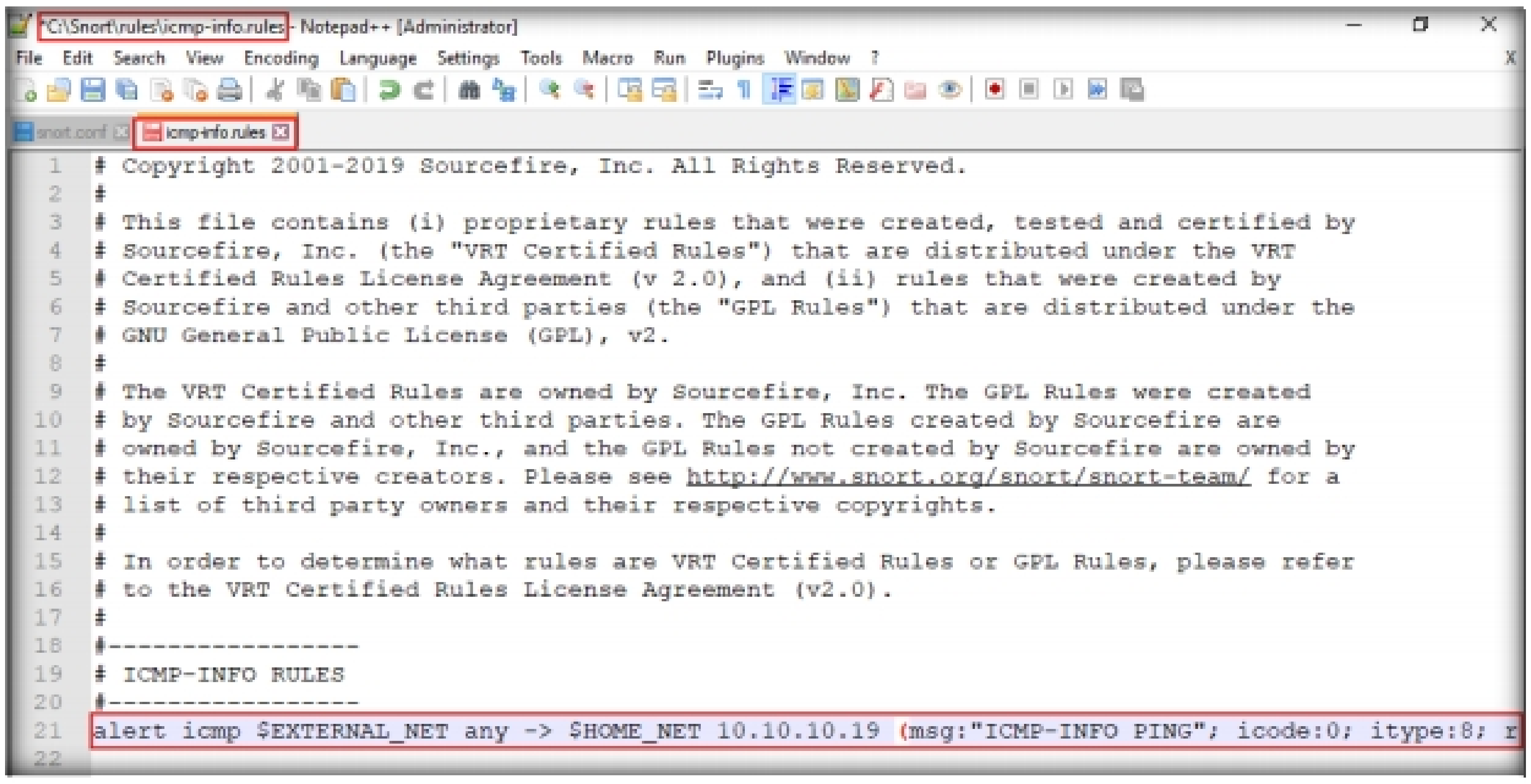
51. Save the **snort.conf** file by pressing **Ctrl+S** and close Notepad++ window.

52. Before running Snort, you need to enable detection rules in the Snort rules file. For this task, we have enabled the ICMP rule so that Snort can detect any host discovery ping probes directed at the system running Snort.

53. Navigate to **C:\Snort\rules** and open the **icmp-info.rules** file with **Notepad ++**.

54. In line 21, type **alert icmp $EXTERNAL_NET any -> $HOME_NET 10.10.10.19 (msg:"ICMP-INFO PING"; icode:0; itype:8; reference:arachnids,135; reference:cve,1999-0265; classtype:bad-unknown; sid:472; rev:7;)** and save. Close the **Notepad++** window.

Note: The IP address (10.10.10.19) mentioned in $HOME_NET may vary in your lab environment.


*C:\Snort\rules\icmp-info.rules - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
snort.conf
icmp-info.rules

```
1  # Copyright 2001-2019 Sourcefire, Inc. All Rights Reserved.
2  #
3  # This file contains (i) proprietary rules that were created, tested and certified by
4  # Sourcefire, Inc. (the "VRT Certified Rules") that are distributed under the VRT
5  # Certified Rules License Agreement (v 2.0), and (ii) rules that were created by
6  # Sourcefire and other third parties (the "GPL Rules") that are distributed under the
7  # GNU General Public License (GPL), v2.
8  #
9  # The VRT Certified Rules are owned by Sourcefire, Inc. The GPL Rules were created
10 # by Sourcefire and other third parties. The GPL Rules created by Sourcefire are
11 # owned by Sourcefire, Inc., and the GPL Rules not created by Sourcefire are owned by
12 # their respective creators. Please see http://www.snort.org/snort/snort-team/ for a
13 # list of third party owners and their respective copyrights.
14 #
15 # In order to determine what rules are VRT Certified Rules or GPL Rules, please refer
16 # to the VRT Certified Rules License Agreement (v2.0).
17 #
18 #-----------------
19 # ICMP-INFO RULES
20 #-----------------
21 alert icmp $EXTERNAL_NET any -> $HOME_NET 10.10.10.19 (msg:"ICMP-INFO PING"; icode:0; itype:8; r
22
```

Figure 1.1.17: Adding a line to ICMP - Info.rules file in Notepad++

TASK 1.4

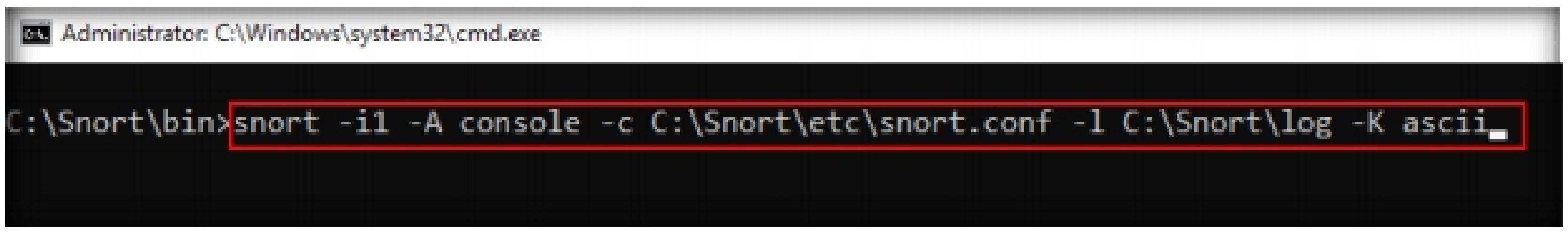
Validate Configurations

55. Now right-click on the **Windows Start** icon and click **Run** from the menu.

56. In the **Run** window, type **cmd** in the **Open** field and press **Enter**. This will launch a command prompt window.

57. In the command prompt window, type **cd C:\Snort\bin** and press **Enter**.

58. Type **snort -iX -A console -c C:\Snort\etc\snort.conf -l C:\Snort\log -K ascii** and press **Enter** to start Snort (replace **X** with your device index number; in this lab: **X** is 1).



```
C:\Snort\bin>snort -i1 -A console -c C:\Snort\etc\snort.conf -l C:\Snort\log -K ascii
```

Figure 1.1.18: Command to activate Snort and save the stored log files

TASK 1.5

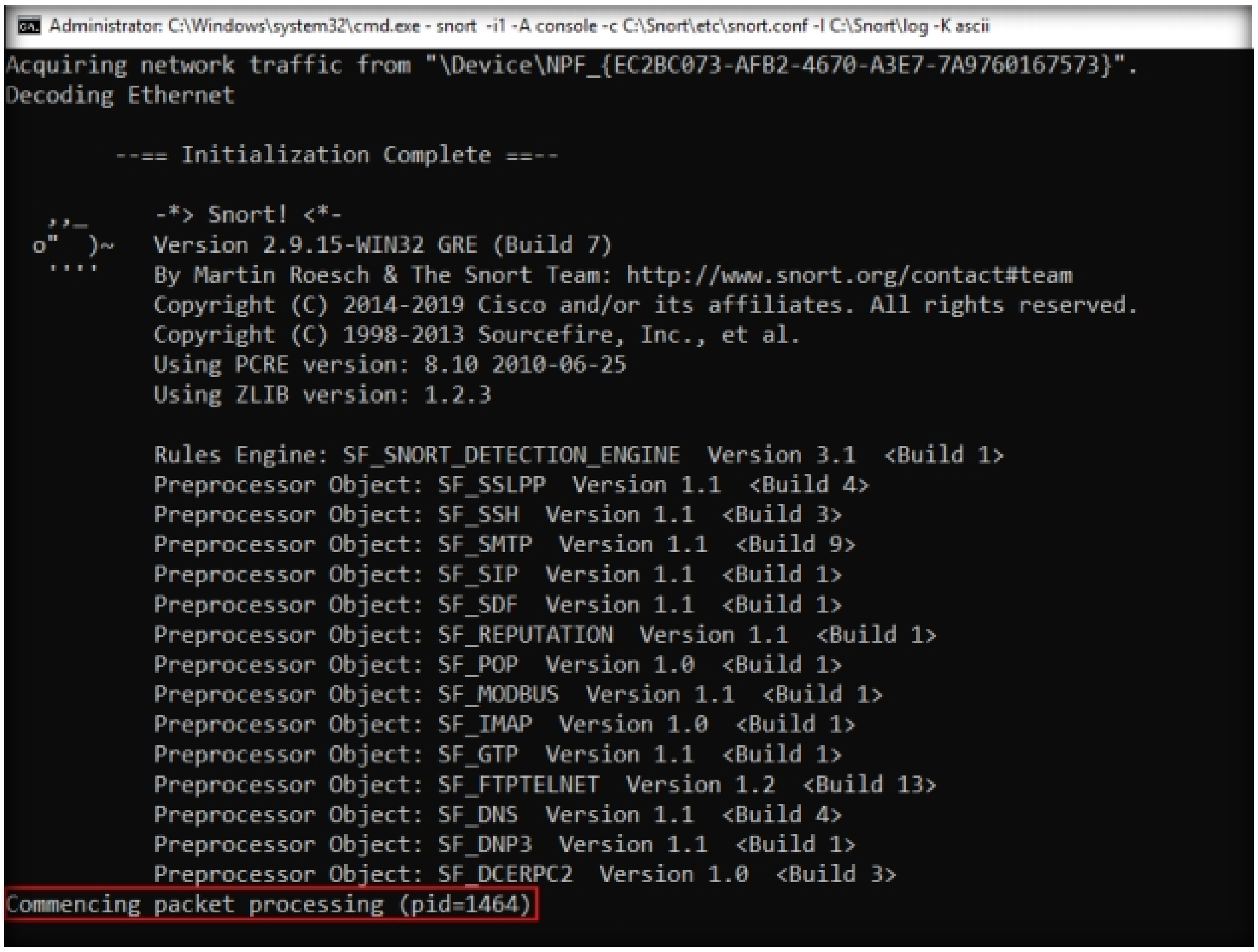
Start Snort

59. If you receive a **fatal error**, you should first **verify** that you have typed all modifications correctly into the **snort.conf** file, and then search through the file for **entries** matching your fatal error message.

60. If you receive an error stating "**Could not create the registry key**," then run the command prompt as **Administrator**.

61. Snort starts running in IDS mode. It first initializes output plug-ins, preprocessors, plug-ins, loads dynamic preprocessors libraries, rule chains of Snort, and then logs all signatures.

62. If you have entered all command information correctly, you receive a comment stating **Commencing packet processing <pid=xxxx>** (the value of xxxx may be any number; in this lab, it is 1464), as shown in the screenshot.



Administrator: C:\Windows\system32\cmd.exe - snort -i1 -A console -c C:\Snort\etc\snort.conf -l C:\Snort\log -K ascii

```
Acquiring network traffic from "\Device\NPF_{EC2BC073-AFB2-4670-A3E7-7A9760167573}".
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.15-WIN32 GRE (Build 7)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.3

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.1  <Build 1>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
Commencing packet processing (pid=1464)
```

Figure 1.1.19: Initializing Snort Rule Chains window

63. After initializing interface and logged signatures, Snort starts and waits for an attack and triggers alerts when attacks occur on the machine.

64. Leave the Snort command prompt running.

65. Attack your own machine, and check whether Snort detects it or not.

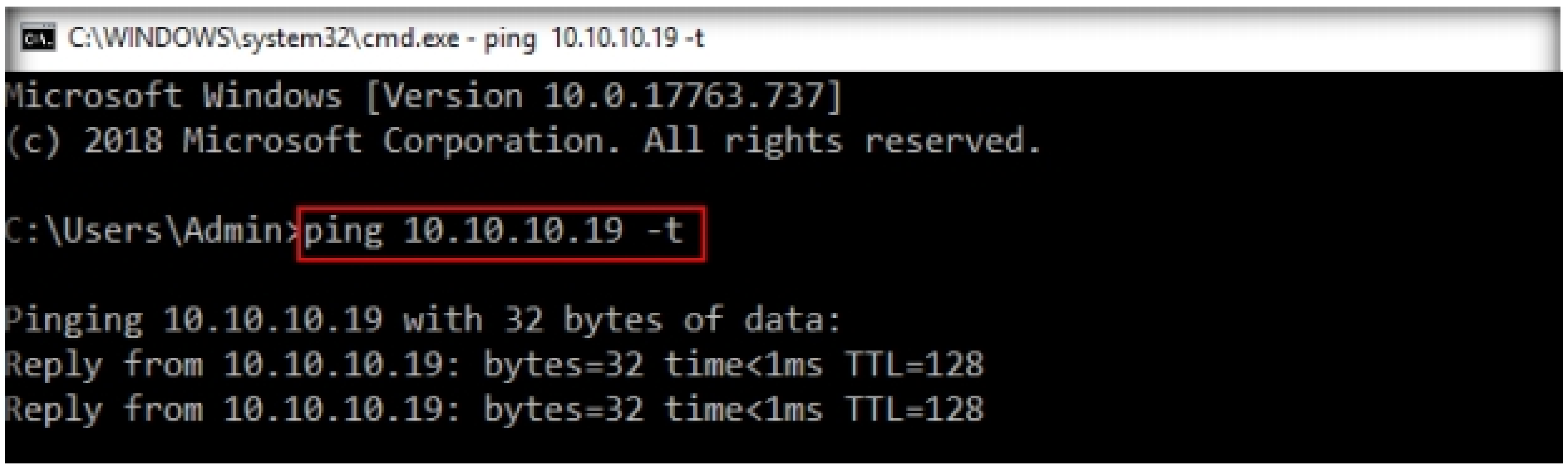
TASK 1.6

Attack Windows Server 2019 Machine

66. Now, switch to the **Windows 10** virtual machine (**Attacker Machine**) and log in with the credentials **Admin** and **Pa$$w0rd**.

67. Open the command prompt and issue the command **ping 10.10.10.19 -t** from the **Attacker Machine**.

Note: **10.10.10.19** is the IP address of the Windows Server 2019. This IP address may differ in your lab environment.

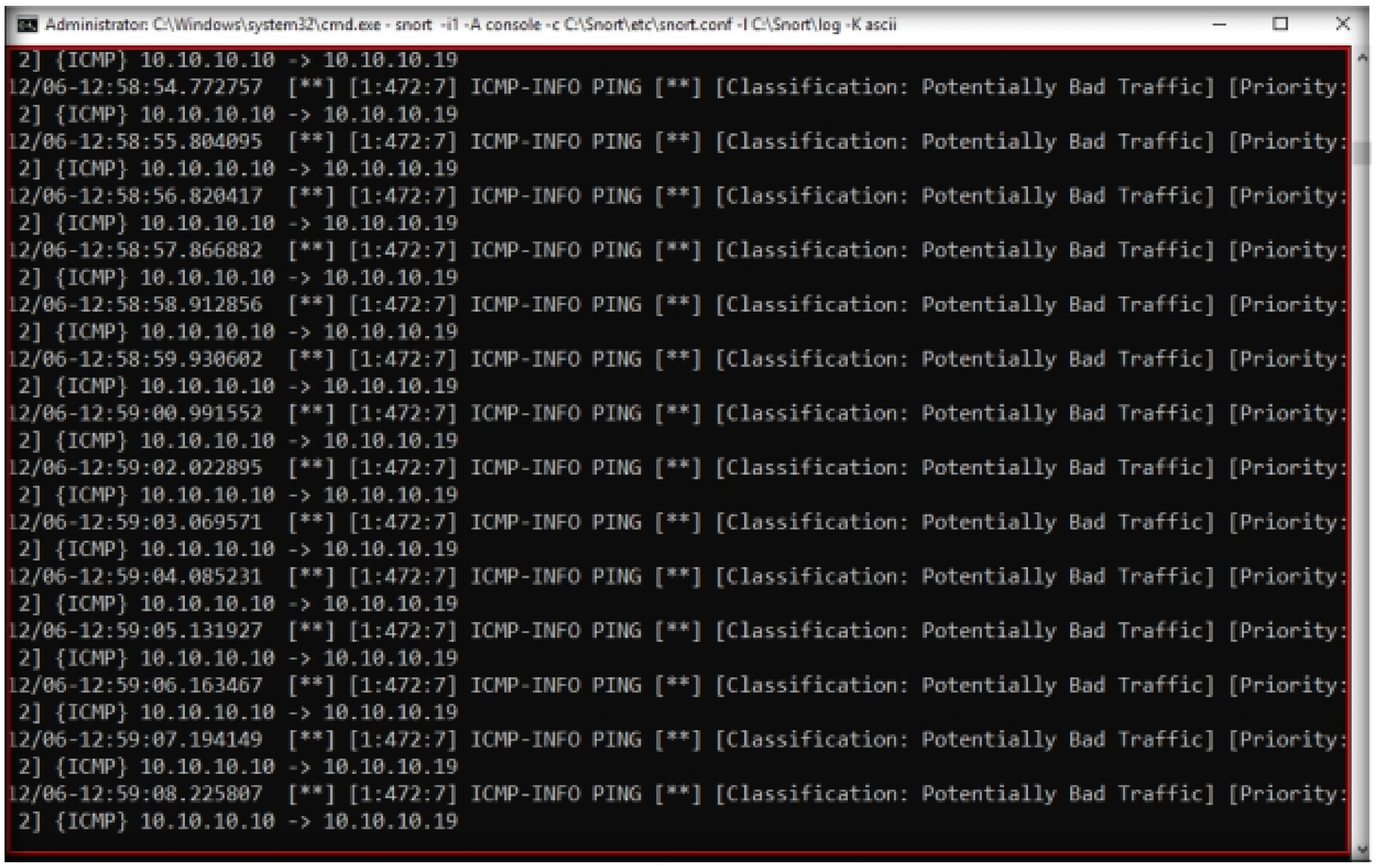


C:\WINDOWS\system32\cmd.exe - ping 10.10.10.19 -t

```
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Admin>ping 10.10.10.19 -t

Pinging 10.10.10.19 with 32 bytes of data:
Reply from 10.10.10.19: bytes=32 time<1ms TTL=128
Reply from 10.10.10.19: bytes=32 time<1ms TTL=128
```

Figure 1.1.20: Pinging the target machine

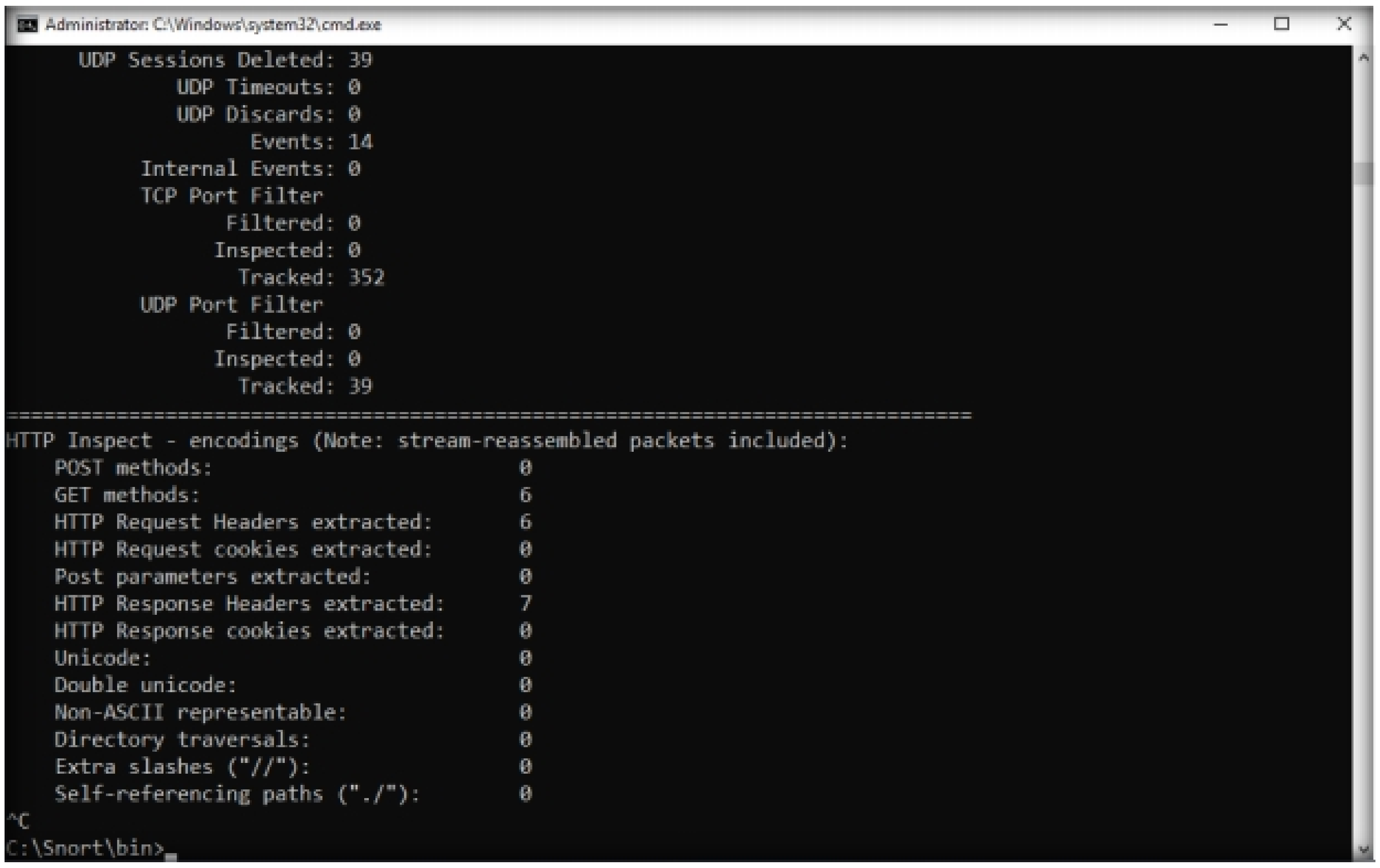
68. Return to the **Windows Server 2019** machine. Observe that Snort triggers an alarm, as shown in the screenshot:


Administrator: C:\Windows\system32\cmd.exe - snort -i1 -A console -c C:\Snort\etc\snort.conf -l C:\Snort\log -K ascii

```
 2] {ICMP} 10.10.10.10 -> 10.10.10.19
12/06-12:58:54.772757  [**] [1:472:7] ICMP-INFO PING [**] [Classification: Potentially Bad Traffic] [Priority:
 2] {ICMP} 10.10.10.10 -> 10.10.10.19
12/06-12:58:55.804095  [**] [1:472:7] ICMP-INFO PING [**] [Classification: Potentially Bad Traffic] [Priority:
 2] {ICMP} 10.10.10.10 -> 10.10.10.19
12/06-12:58:56.820417  [**] [1:472:7] ICMP-INFO PING [**] [Classification: Potentially Bad Traffic] [Priority:
 2] {ICMP} 10.10.10.10 -> 10.10.10.19
12/06-12:58:57.866882  [**] [1:472:7] ICMP-INFO PING [**] [Classification: Potentially Bad Traffic] [Priority:
 2] {ICMP} 10.10.10.10 -> 10.10.10.19
12/06-12:58:58.912856  [**] [1:472:7] ICMP-INFO PING [**] [Classification: Potentially Bad Traffic] [Priority:
 2] {ICMP} 10.10.10.10 -> 10.10.10.19
12/06-12:58:59.930602  [**] [1:472:7] ICMP-INFO PING [**] [Classification: Potentially Bad Traffic] [Priority:
 2] {ICMP} 10.10.10.10 -> 10.10.10.19
12/06-12:59:00.991552  [**] [1:472:7] ICMP-INFO PING [**] [Classification: Potentially Bad Traffic] [Priority:
 2] {ICMP} 10.10.10.10 -> 10.10.10.19
12/06-12:59:02.022895  [**] [1:472:7] ICMP-INFO PING [**] [Classification: Potentially Bad Traffic] [Priority:
 2] {ICMP} 10.10.10.10 -> 10.10.10.19
12/06-12:59:03.069571  [**] [1:472:7] ICMP-INFO PING [**] [Classification: Potentially Bad Traffic] [Priority:
 2] {ICMP} 10.10.10.10 -> 10.10.10.19
12/06-12:59:04.085231  [**] [1:472:7] ICMP-INFO PING [**] [Classification: Potentially Bad Traffic] [Priority:
 2] {ICMP} 10.10.10.10 -> 10.10.10.19
12/06-12:59:05.131927  [**] [1:472:7] ICMP-INFO PING [**] [Classification: Potentially Bad Traffic] [Priority:
 2] {ICMP} 10.10.10.10 -> 10.10.10.19
12/06-12:59:06.163467  [**] [1:472:7] ICMP-INFO PING [**] [Classification: Potentially Bad Traffic] [Priority:
 2] {ICMP} 10.10.10.10 -> 10.10.10.19
12/06-12:59:07.194149  [**] [1:472:7] ICMP-INFO PING [**] [Classification: Potentially Bad Traffic] [Priority:
 2] {ICMP} 10.10.10.10 -> 10.10.10.19
12/06-12:59:08.225807  [**] [1:472:7] ICMP-INFO PING [**] [Classification: Potentially Bad Traffic] [Priority:
 2] {ICMP} 10.10.10.10 -> 10.10.10.19
```

Figure 1.1.21: Snort alerts

69. Press **Ctrl+C** to **stop** Snort; snort exits.



```
     UDP Sessions Deleted: 39
             UDP Timeouts: 0
             UDP Discards: 0
                   Events: 14
          Internal Events: 0
          TCP Port Filter
                Filtered: 0
               Inspected: 0
                 Tracked: 352
          UDP Port Filter
                Filtered: 0
               Inspected: 0
                 Tracked: 39
===============================================================================
HTTP Inspect - encodings (Note: stream-reassembled packets included):
    POST methods:                         0
    GET methods:                          6
    HTTP Request Headers extracted:       6
    HTTP Request cookies extracted:       0
    Post parameters extracted:            0
    HTTP Response Headers extracted:      7
    HTTP Response cookies extracted:      0
    Unicode:                              0
    Double unicode:                       0
    Non-ASCII representable:              0
    Directory traversals:                 0
    Extra slashes ("//"):                 0
    Self-referencing paths ("./"):        0
^C
C:\Snort\bin>_
```

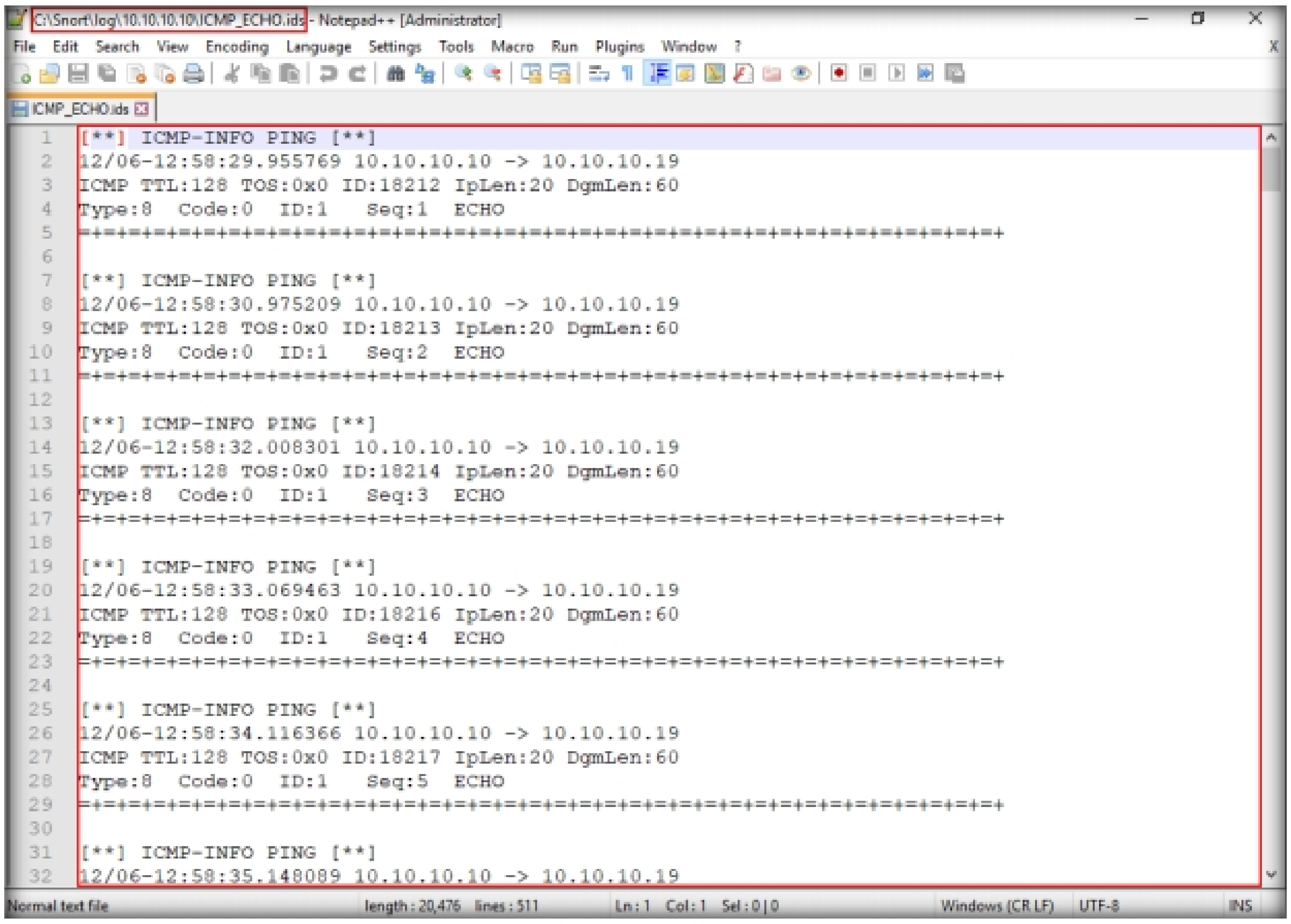
Figure 1.1.22: Exiting Snort by pressing Ctrl+C

TASK 1.7

Examine Log File

70. Go to the **C:\Snort\log\10.10.10.10** folder and open the **ICMP_ECHO.ids** file with **Notepad++**. You see that all the log entries are saved in the **ICMP_ECHO.ids** file.

Note: The folder name **10.10.10.10** might vary in your lab environment, depending on the IP address of the **Windows 10** machine.


C:\Snort\log\10.10.10.10\ICMP_ECHO.ids - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
ICMP_ECHO.ids
Normal text file
length : 20,476 lines : 511
Ln : 1 Col : 1 Sel : 0 | 0
Windows (CR LF)
UTF-8
INS

```
[**] ICMP-INFO PING [**]
12/06-12:58:29.955769 10.10.10.10 -> 10.10.10.19
ICMP TTL:128 TOS:0x0 ID:18212 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:1  ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] ICMP-INFO PING [**]
12/06-12:58:30.975209 10.10.10.10 -> 10.10.10.19
ICMP TTL:128 TOS:0x0 ID:18213 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:2  ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] ICMP-INFO PING [**]
12/06-12:58:32.008301 10.10.10.10 -> 10.10.10.19
ICMP TTL:128 TOS:0x0 ID:18214 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:3  ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] ICMP-INFO PING [**]
12/06-12:58:33.069463 10.10.10.10 -> 10.10.10.19
ICMP TTL:128 TOS:0x0 ID:18216 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:4  ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] ICMP-INFO PING [**]
12/06-12:58:34.116366 10.10.10.10 -> 10.10.10.19
ICMP TTL:128 TOS:0x0 ID:18217 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:5  ECHO
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] ICMP-INFO PING [**]
12/06-12:58:35.148089 10.10.10.10 -> 10.10.10.19
```

Figure 1.1.23: Saved Snort logs

Note: This means that whenever an attacker attempts to connect or communicate with the machine, Snort immediately triggers an alarm.

Note: This will make you aware of the intrusion and can thus take certain security measures to disconnect the lines of communication with the attacker's machine.

71. Close all open windows in the **Windows 10** and **Windows Server 2019** virtual machines and shut down the **Windows Server 2019** virtual machine.

TASK 2

Detect Malicious Network Traffic using ZoneAlarm FREE FIREWALL 2019

Note: Ensure that the **Windows 10** virtual machine is running.

1. Launch the **Windows Server 2019** virtual machine.
2. Before starting this task, we will browse an unwanted website in the **Windows 10** machine. Assume that **www.moviescope.com** is an unwanted site that is not supposed to be browsed in your network.

Note: **www.moviescope.com** is a local website that is hosted and configured in the **Windows Server 2019** machine.

3. In the **Windows 10** machine, open any browser (here, **Google Chrome**) and type **www.moviescope.com** in the address bar and press **Enter**.

ZoneAlarm FREE Firewall 2019 blocks attackers and intruders from accessing your system. It manages and monitors all incoming and outgoing traffic and shields the network from hackers, malware, and other online threats that put network privacy at risk, and monitors programs for suspicious behavior spotting and stopping new attacks that bypass traditional anti-virus protection.

4. As you can observe that **www.moviescope.com** can be browsed in the **Windows 10** machine.

TASK 2.1

Browse MovieScope Website

5. In this task, we are going to block this site from browsing. Close the **Google Chrome** browser.

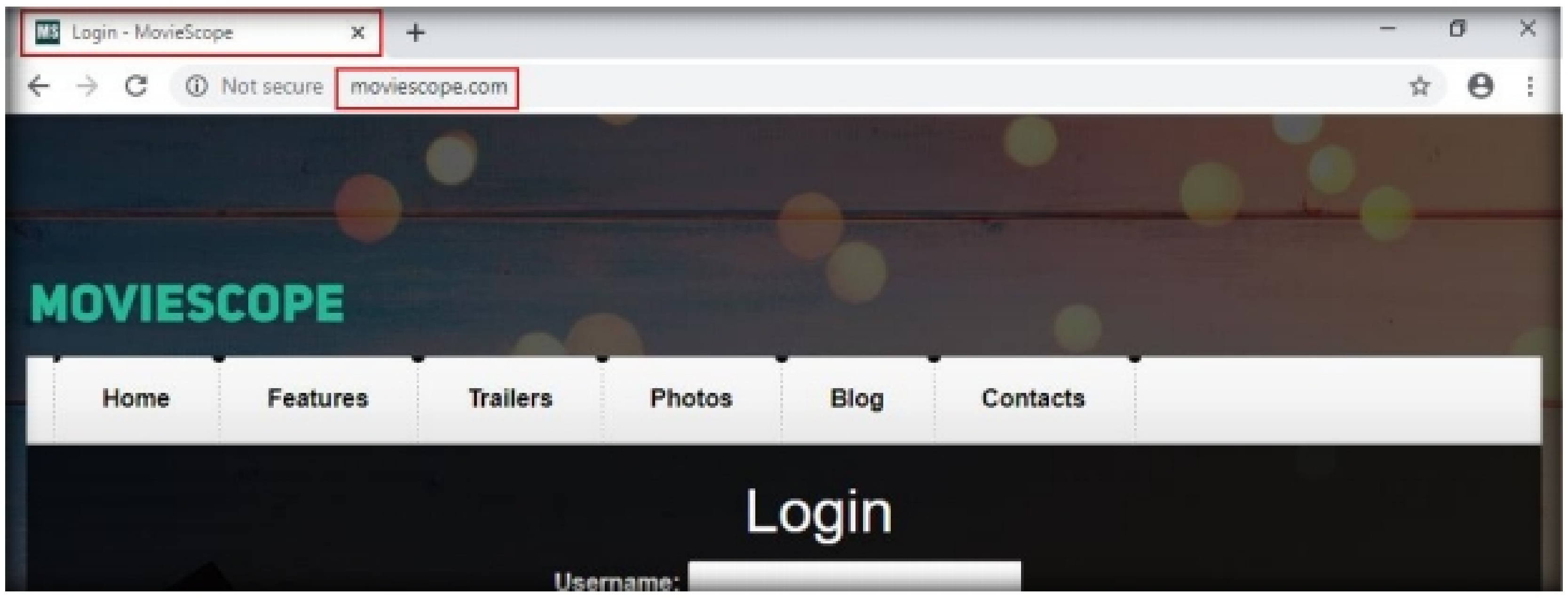

Login - MovieScope
Not secure
moviescope.com
MOVIESCOPE
Home
Features
Trailers
Photos
Blog
Contacts
Login
Username:

Figure 1.2.1: www.moviescope.com site accessible

TASK 2.2

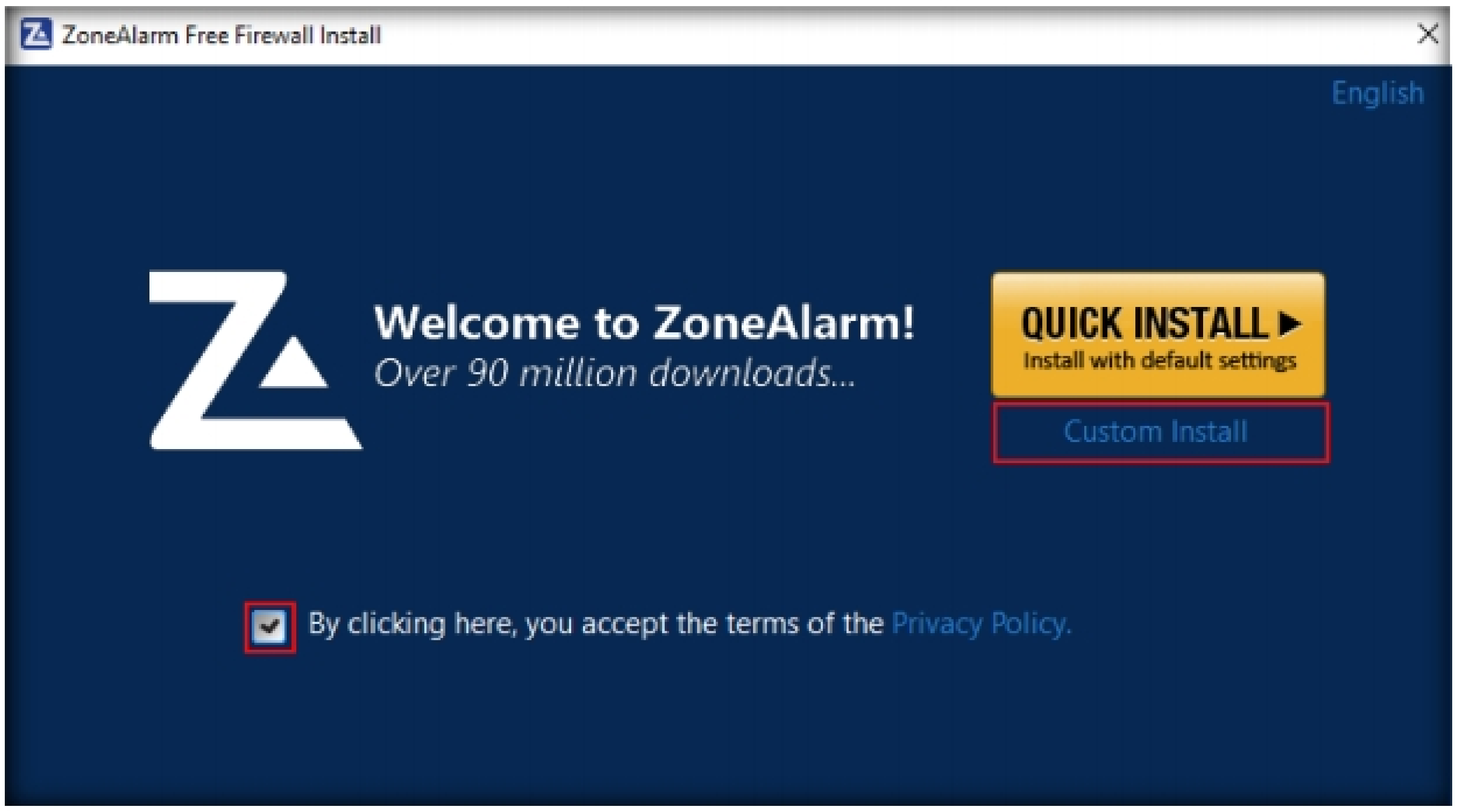
Install ZoneAlarm Firewall

ZoneAlarm FREE Firewall 2019 prevents identity theft by guarding your data, and erases your tracks allowing you to surf the web in complete privacy. Furthermore, it locks out attackers, blocks intrusions, and makes your PC invisible online. Additionally, it filters out annoying, as well as potentially dangerous, email.

6. In the **Windows 10** machine, navigate to **E:\CEH-Tools\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots\Firewalls\ZoneAlarm FREE FIREWALL 2019** and double-click **zafwSetupWeb_158_023_18219.exe** to install ZoneAlarm FREE FIREWALL 2019.

7. If the **User Account Control** pop-up appears, click **Yes**.

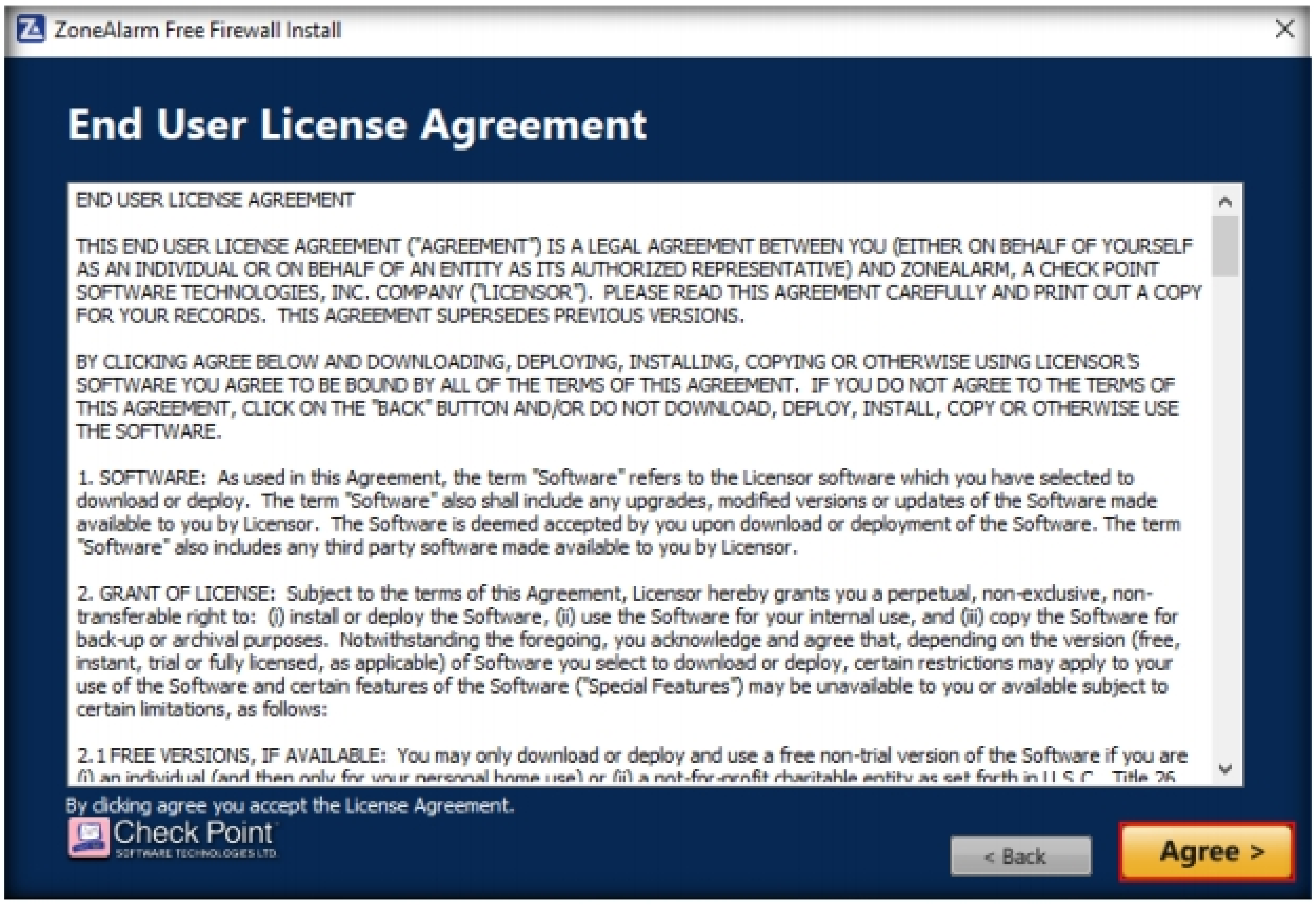
8. The **ZoneAlarm Free Firewall Install** wizard appears; check **By clicking here, you accept the terms of the Privacy Policy**, and then click **Custom Install**.


ZoneAlarm Free Firewall Install
English
Welcome to ZoneAlarm!
Over 90 million downloads...
QUICK INSTALL ▶
Install with default settings
Custom Install

☑ By clicking here, you accept the terms of the Privacy Policy.

Figure 1.2.2: ZoneAlarm Custom Install

9. The **End User License Agreement** wizard appears; click **Agree >**.


ZoneAlarm Free Firewall Install
Check Point SOFTWARE TECHNOLOGIES LTD
< Back
Agree >

End User License Agreement

END USER LICENSE AGREEMENT

THIS END USER LICENSE AGREEMENT ("AGREEMENT") IS A LEGAL AGREEMENT BETWEEN YOU (EITHER ON BEHALF OF YOURSELF AS AN INDIVIDUAL OR ON BEHALF OF AN ENTITY AS ITS AUTHORIZED REPRESENTATIVE) AND ZONEALARM, A CHECK POINT SOFTWARE TECHNOLOGIES, INC. COMPANY ("LICENSOR"). PLEASE READ THIS AGREEMENT CAREFULLY AND PRINT OUT A COPY FOR YOUR RECORDS. THIS AGREEMENT SUPERSEDES PREVIOUS VERSIONS.

BY CLICKING AGREE BELOW AND DOWNLOADING, DEPLOYING, INSTALLING, COPYING OR OTHERWISE USING LICENSOR'S SOFTWARE YOU AGREE TO BE BOUND BY ALL OF THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, CLICK ON THE "BACK" BUTTON AND/OR DO NOT DOWNLOAD, DEPLOY, INSTALL, COPY OR OTHERWISE USE THE SOFTWARE.

1. SOFTWARE: As used in this Agreement, the term "Software" refers to the Licensor software which you have selected to download or deploy. The term "Software" also shall include any upgrades, modified versions or updates of the Software made available to you by Licensor. The Software is deemed accepted by you upon download or deployment of the Software. The term "Software" also includes any third party software made available to you by Licensor.

2. GRANT OF LICENSE: Subject to the terms of this Agreement, Licensor hereby grants you a perpetual, non-exclusive, non-transferable right to: (i) install or deploy the Software, (ii) use the Software for your internal use, and (iii) copy the Software for back-up or archival purposes. Notwithstanding the foregoing, you acknowledge and agree that, depending on the version (free, instant, trial or fully licensed, as applicable) of Software you select to download or deploy, certain restrictions may apply to your use of the Software and certain features of the Software ("Special Features") may be unavailable to you or available subject to certain limitations, as follows:

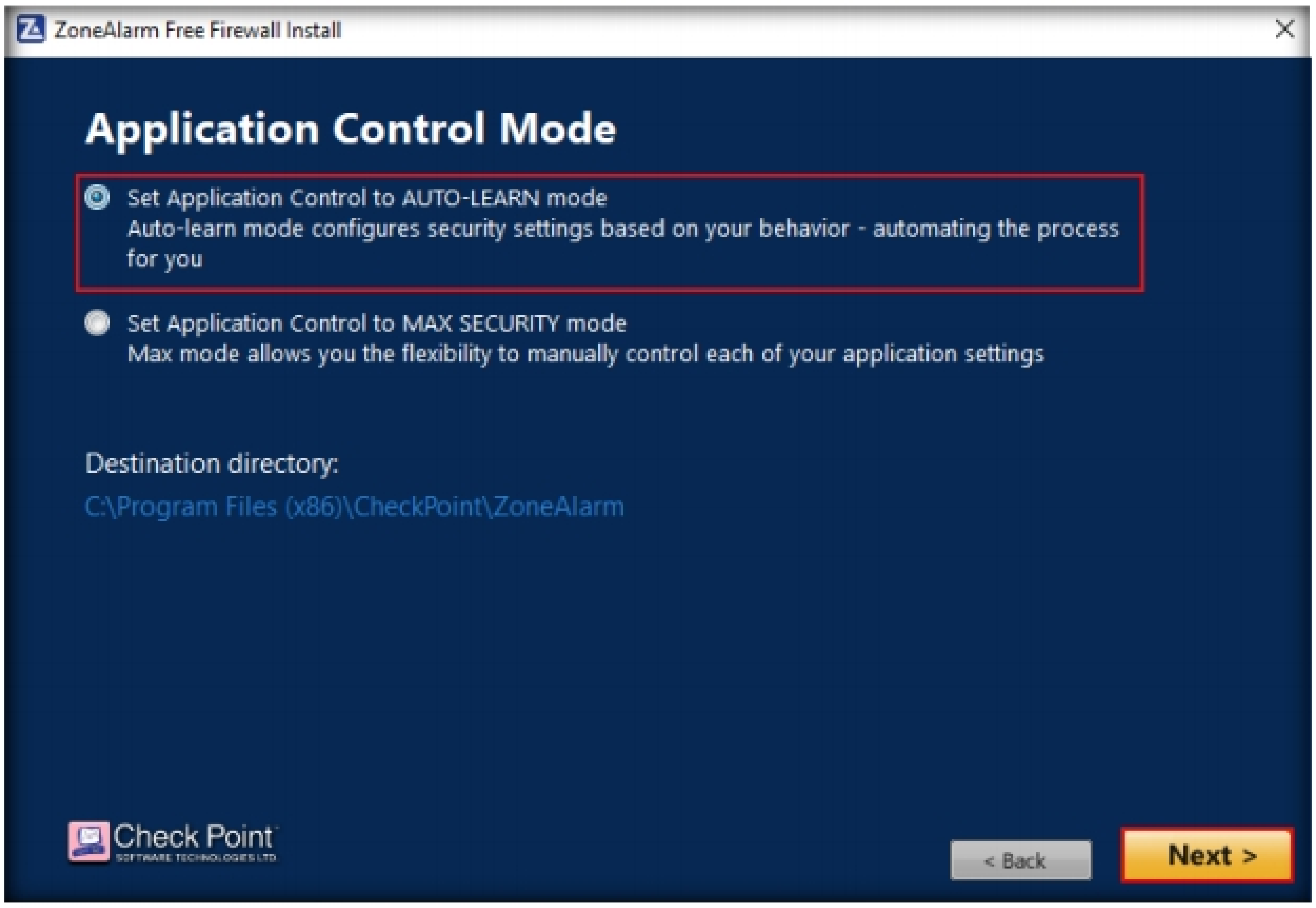
2.1 FREE VERSIONS, IF AVAILABLE: You may only download or deploy and use a free non-trial version of the Software if you are (i) an individual (and then only for your personal home use) or (ii) a not-for-profit charitable entity as set forth in U.S.C. Title 26

By clicking agree you accept the License Agreement.

Figure 1.2.3: ZoneAlarm License Agreement

10. In the **Application Control Mode** wizard, ensure that the **Set Application Control to AUTO-LEARN mode** option is selected, and click **Next >**.

11. By choosing this mode, Zone Alarm Firewall configures the security settings based on behavior and automates this process for your network.


ZoneAlarm Free Firewall Install
Check Point SOFTWARE TECHNOLOGIES LTD
< Back
Next >

Application Control Mode

● Set Application Control to AUTO-LEARN mode
Auto-learn mode configures security settings based on your behavior - automating the process for you

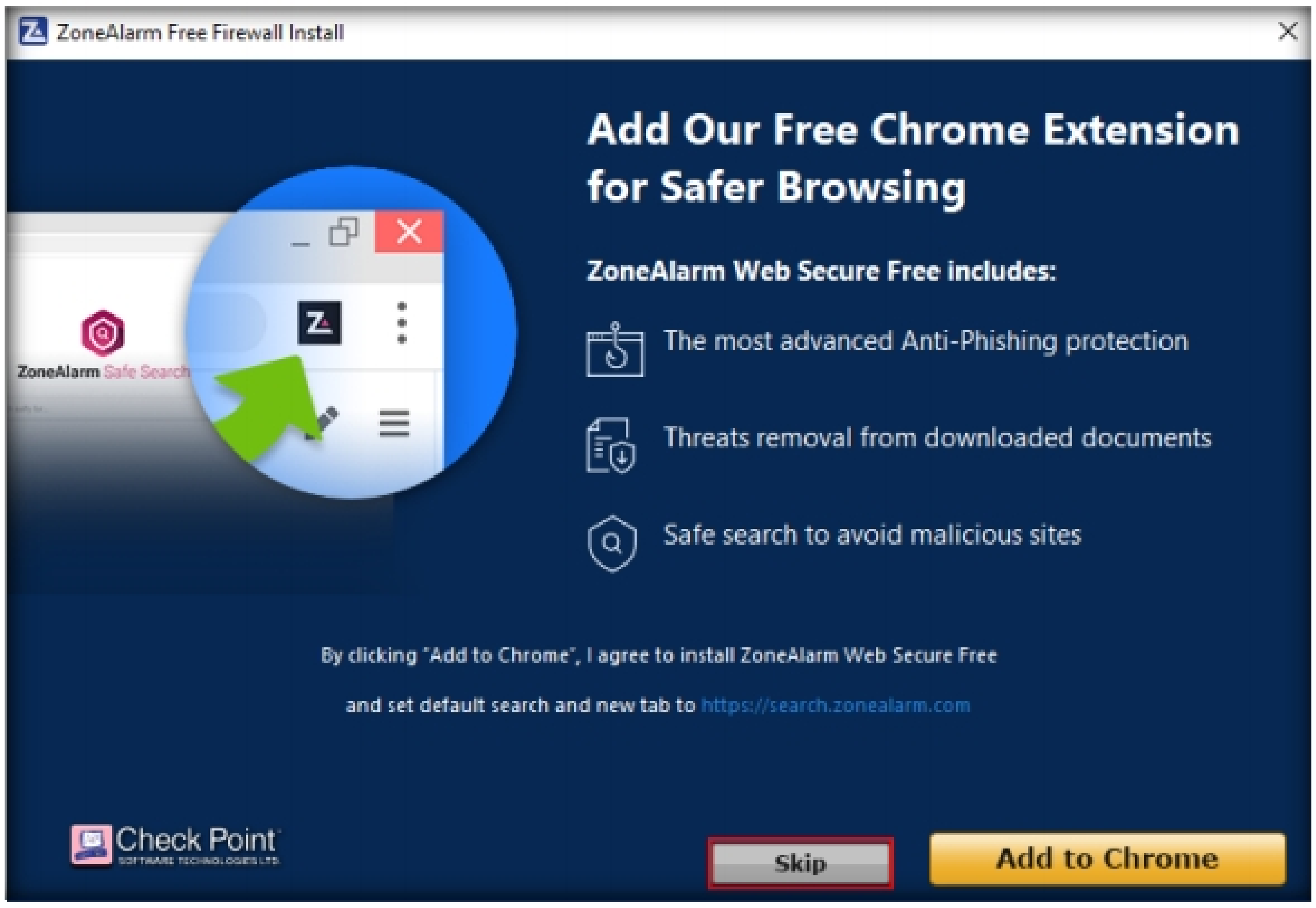
○ Set Application Control to MAX SECURITY mode
Max mode allows you the flexibility to manually control each of your application settings

Destination directory:
C:\Program Files (x86)\CheckPoint\ZoneAlarm

Figure 1.2.4: ZoneAlarm Application Control Mode

12. Click the **Skip** button in the **Add our Free Chrome Extension for Safer Browsing** wizard.

Note: If you wish to enable this option, click **Add to Chrome**. In this task, we are choosing to skip this option.



ZoneAlarm Free Firewall Install

Add Our Free Chrome Extension for Safer Browsing

ZoneAlarm Web Secure Free includes:

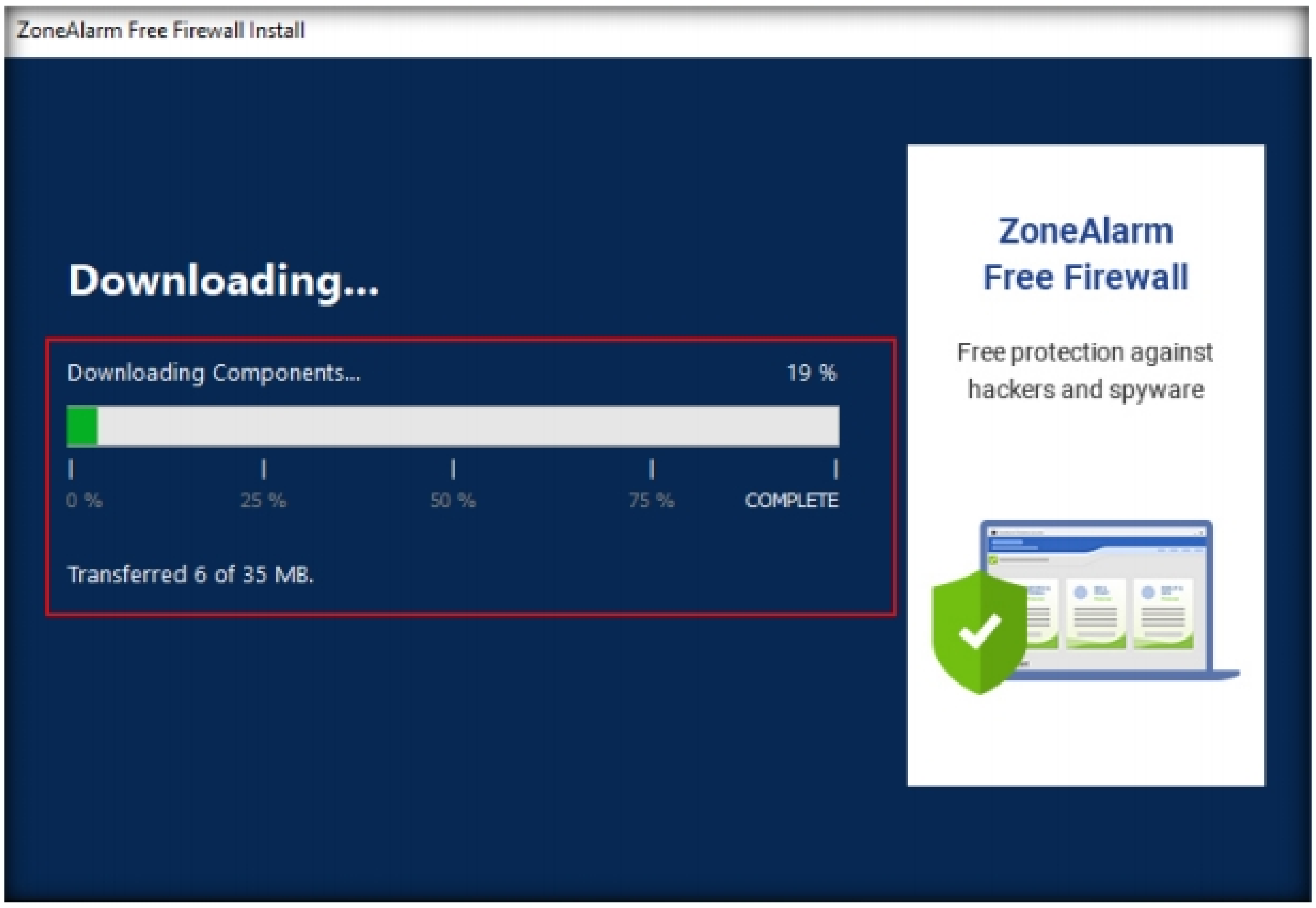
- The most advanced Anti-Phishing protection
- Threats removal from downloaded documents
- Safe search to avoid malicious sites

By clicking "Add to Chrome", I agree to install ZoneAlarm Web Secure Free and set default search and new tab to https://search.zonealarm.com

Figure 1.2.5: ZoneAlarm Chrome Extension

13. ZoneAlarm Free Firewall starts downloading and configuring the components to your machine.

14. Wait until the installation is completed: this may take a few minutes to install.



ZoneAlarm Free Firewall Install

Downloading...

Downloading Components... 19 %

Transferred 6 of 35 MB.

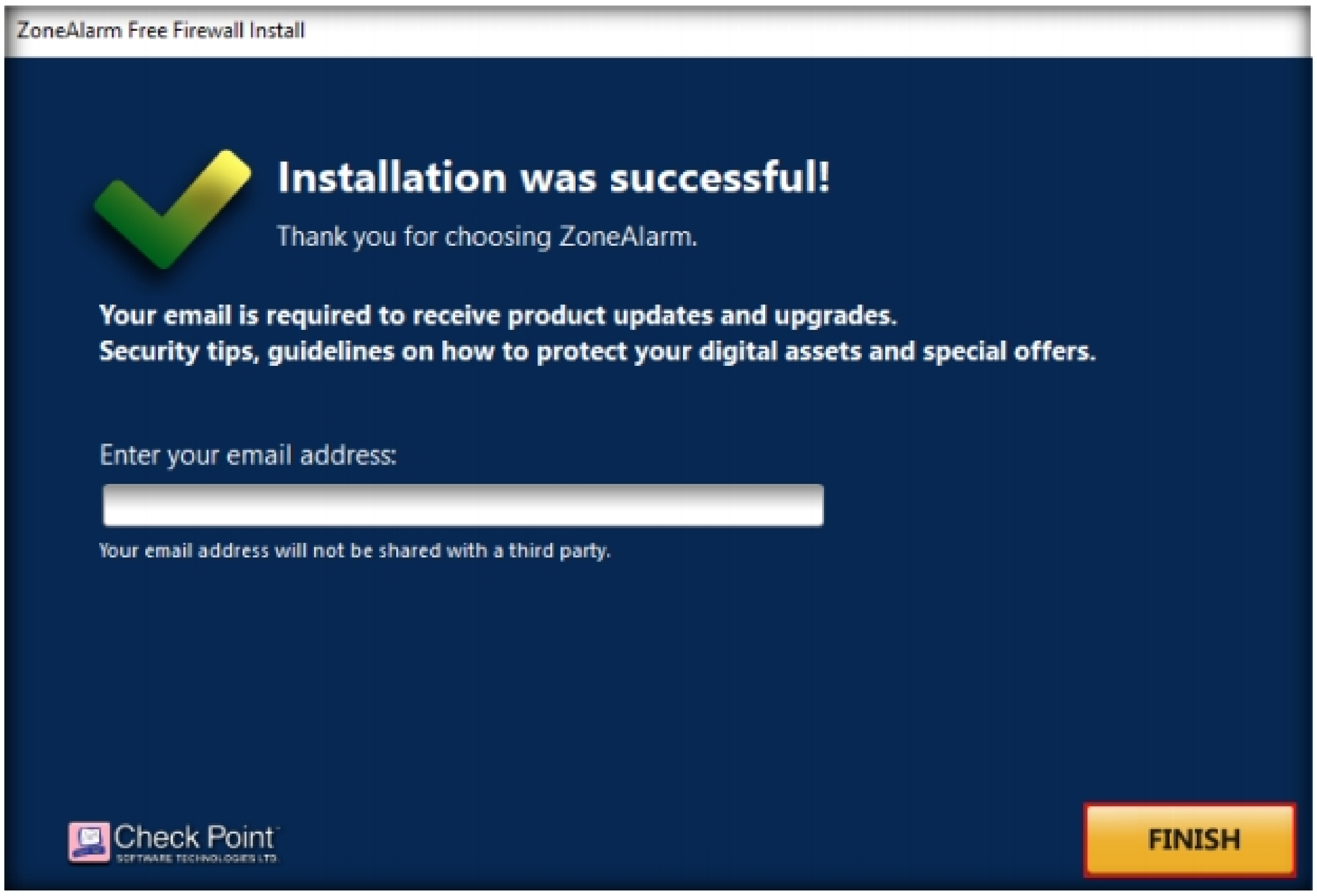
ZoneAlarm Free Firewall

Free protection against hackers and spyware

Figure 1.2.6: ZoneAlarm Downloading Components

15. The **Installation was Successful!** wizard appears; click **FINISH**.

16. As soon as you click the **Finish** button, the ZoneAlarm webpage opens in your default browser window; close the browser.


ZoneAlarm Free Firewall Install

Installation was successful!

Thank you for choosing ZoneAlarm.

Your email is required to receive product updates and upgrades.
Security tips, guidelines on how to protect your digital assets and special offers.

Enter your email address:

Your email address will not be shared with a third party.

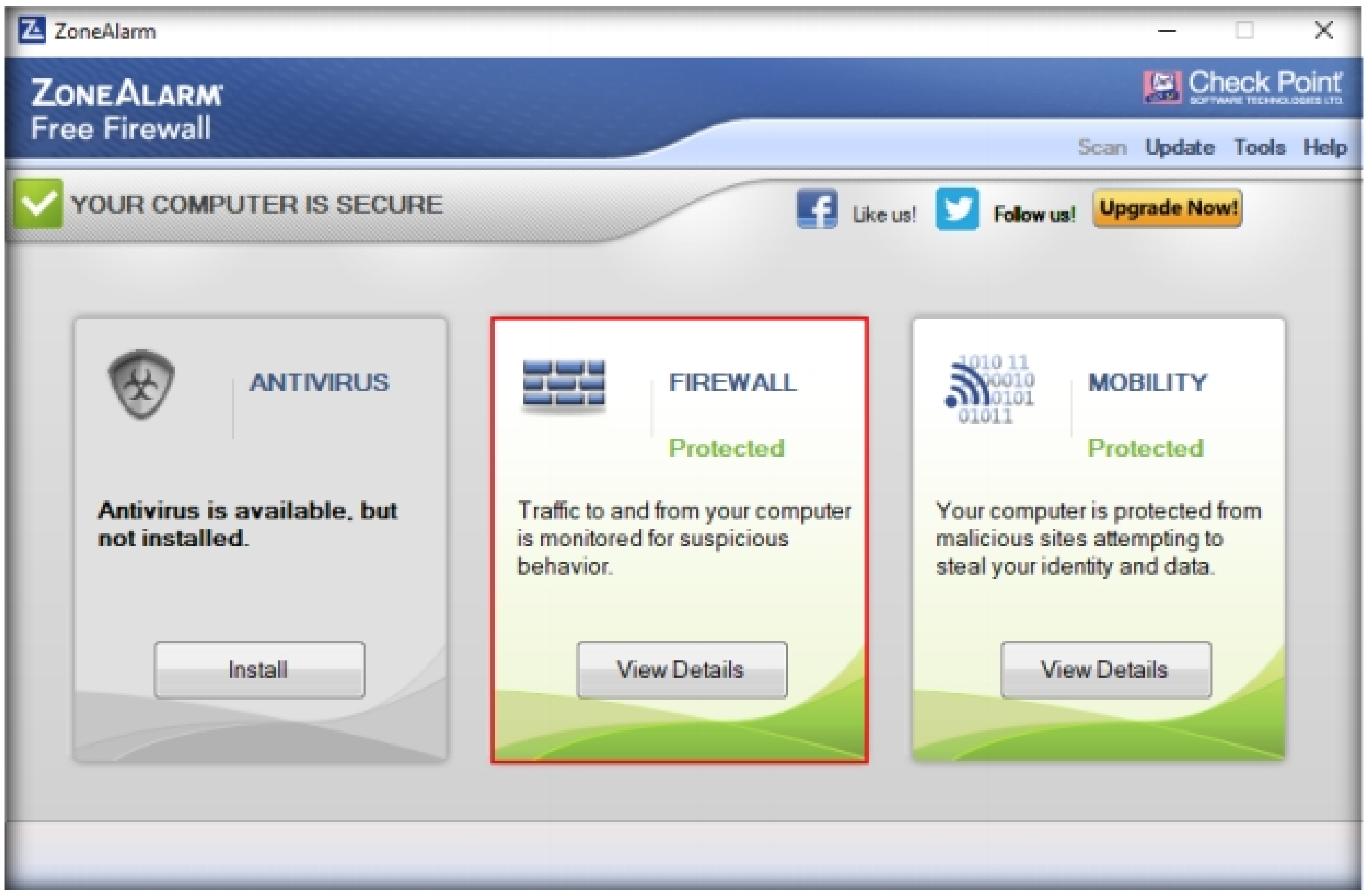
Check Point
FINISH

Figure 1.2.7: ZoneAlarm installation success

TASK 2.3

Configure ZoneAlarm Firewall

17. The **ZoneAlarm** main window appears, as shown in the screenshot. Click the **FIREWALL** button to configure the firewall settings.


ZoneAlarm
ZONEALARM
Free Firewall
Check Point
Scan
Update
Tools
Help
YOUR COMPUTER IS SECURE
Like us!
Follow us!
Upgrade Now!
ANTIVIRUS
Install
FIREWALL
Protected
View Details
MOBILITY
Protected
View Details

Antivirus is available, but not installed.

Traffic to and from your computer is monitored for suspicious behavior.

Your computer is protected from malicious sites attempting to steal your identity and data.

Figure 1.2.8: ZoneAlarm main window

18. In the **FIREWALL** tab, click **View Zones** under the **Basic Firewall** section.

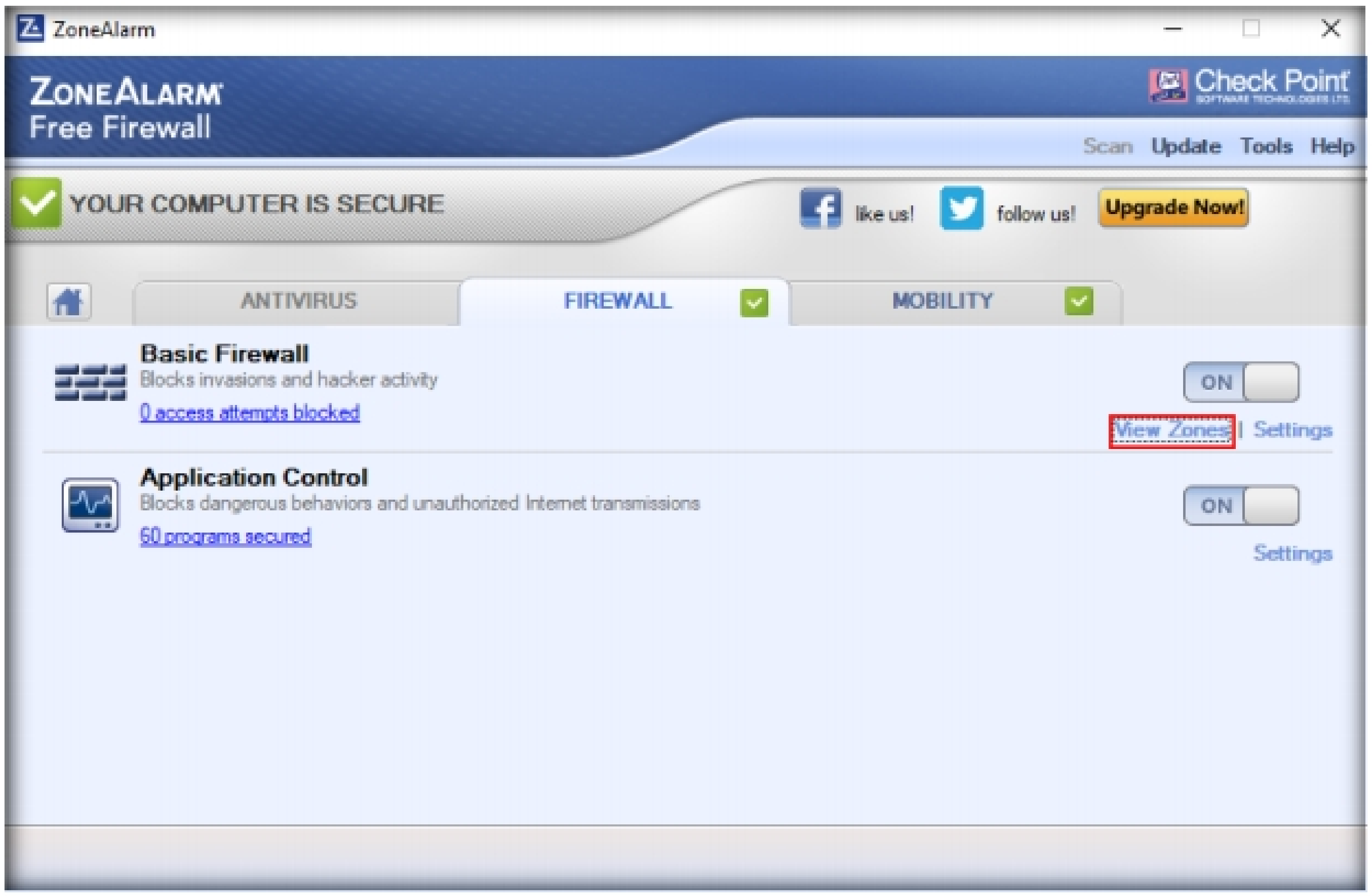
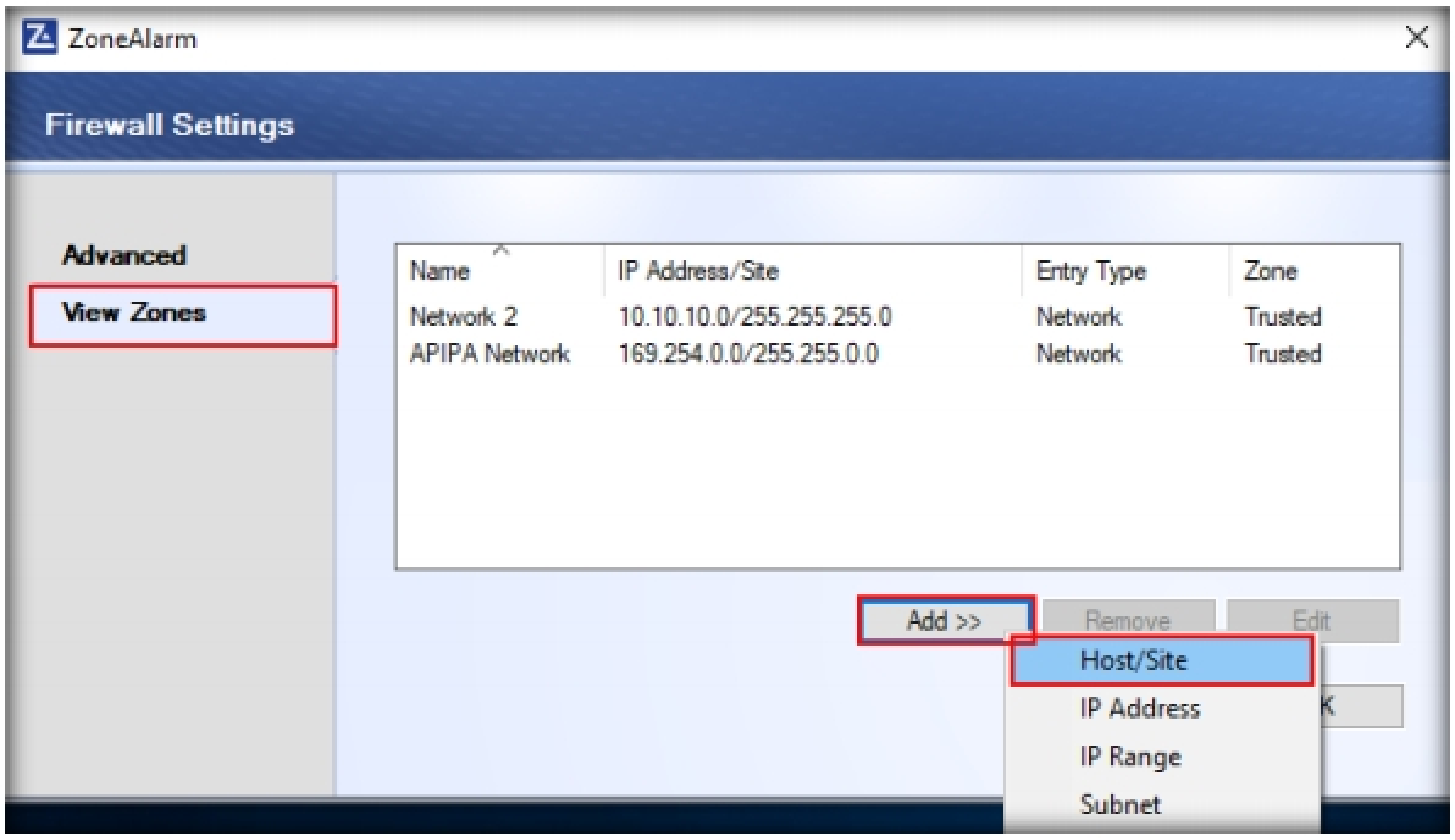

ZoneAlarm
ZONEALARM
Free Firewall
Check Point
Scan
Update
Tools
Help
YOUR COMPUTER IS SECURE
like us!
follow us!
Upgrade Now!
ANTIVIRUS
FIREWALL
MOBILITY
Basic Firewall
Blocks invasions and hacker activity
0 access attempts blocked
ON
View Zones
Settings
Application Control
Blocks dangerous behaviors and unauthorized Internet transmissions
60 programs secured
ON
Settings

Figure 1.2.9: ZoneAlarm Firewall settings

TASK 2.4

View Zones

19. The **Firewall Settings** window appears with the **View Zones** tab selected; click **Add >>** and click the **Host/Site** option from the menu, as shown in the screenshot.


ZoneAlarm
Firewall Settings
Advanced
View Zones
Add >>
Remove
Edit
Host/Site
IP Address
IP Range
Subnet

Name	IP Address/Site	Entry Type	Zone
Network 2	10.10.10.0/255.255.255.0	Network	Trusted
APIPA Network	169.254.0.0/255.255.0.0	Network	Trusted

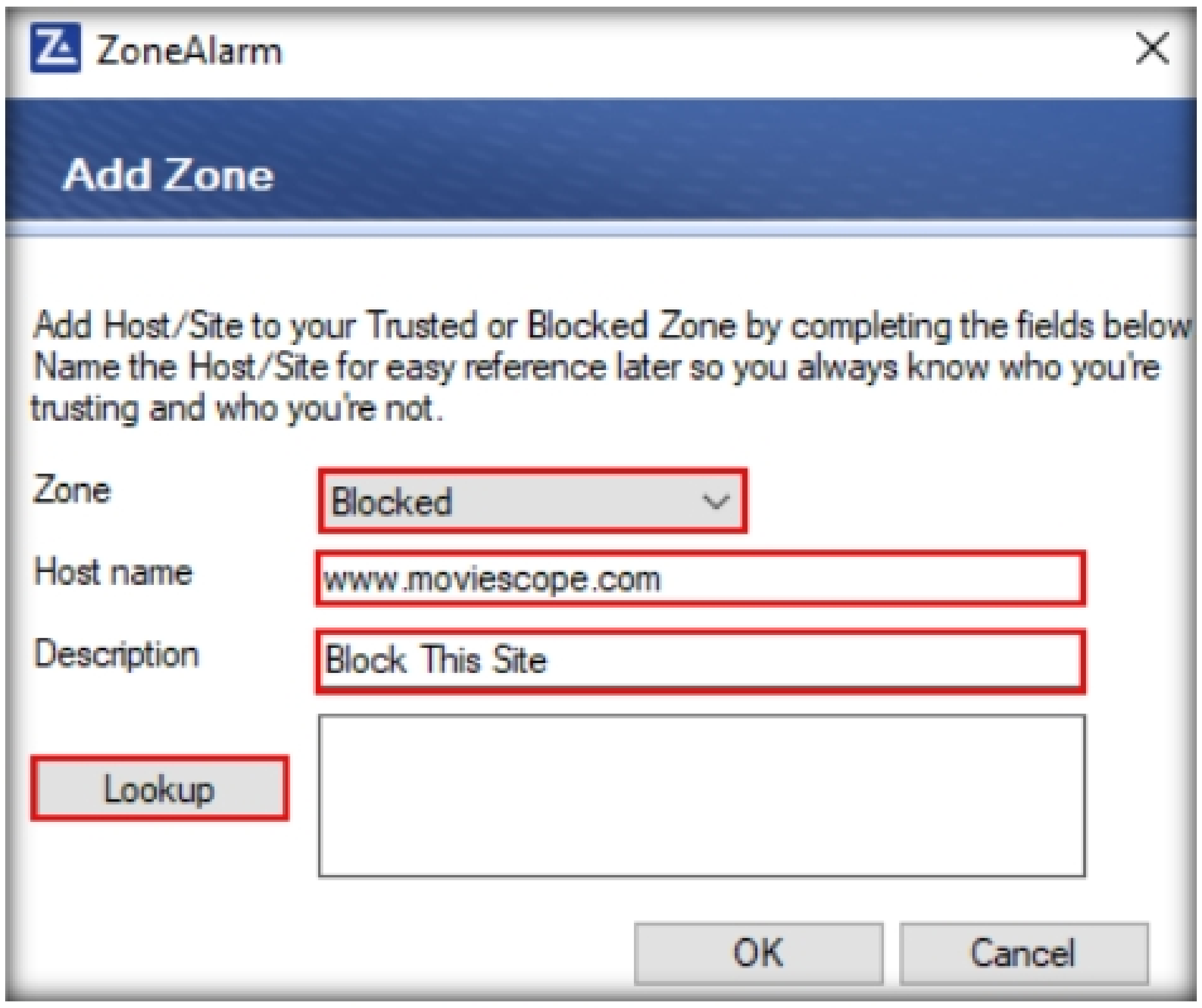
Figure 1.2.10: ZoneAlarm View Zones

20. The **Add Zone** window appears; choose the following:
    a. Zone: **Blocked**
    b. Hostname: **www.moviescope.com**
    c. Description: **Block This Site**

   d. Click **Lookup**; by doing this, we are blocking unwanted sites from browsing

21. You can provide any site that you wish to block.

Note: **www.moviescope.com** is the local website that is configured on Windows Server 2019.

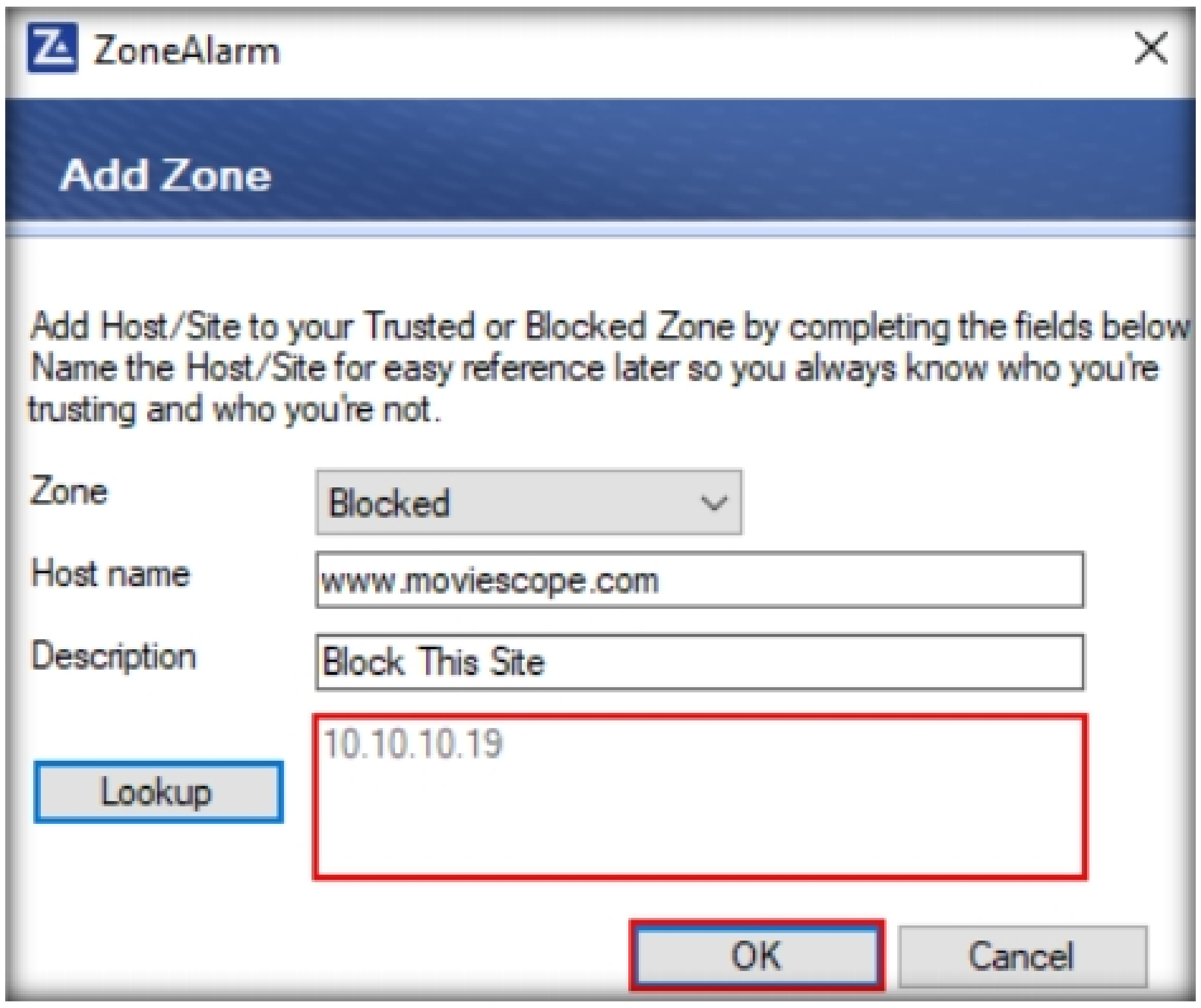


Add Host/Site to your Trusted or Blocked Zone by completing the fields below Name the Host/Site for easy reference later so you always know who you're trusting and who you're not.

Zone: Blocked
Host name: www.moviescope.com
Description: Block This Site

Figure 1.2.11: ZoneAlarm Adding Zone

22. As soon as you click **Lookup**, the IP address of **www.moviescope.com** appears in the text field; click **OK**.

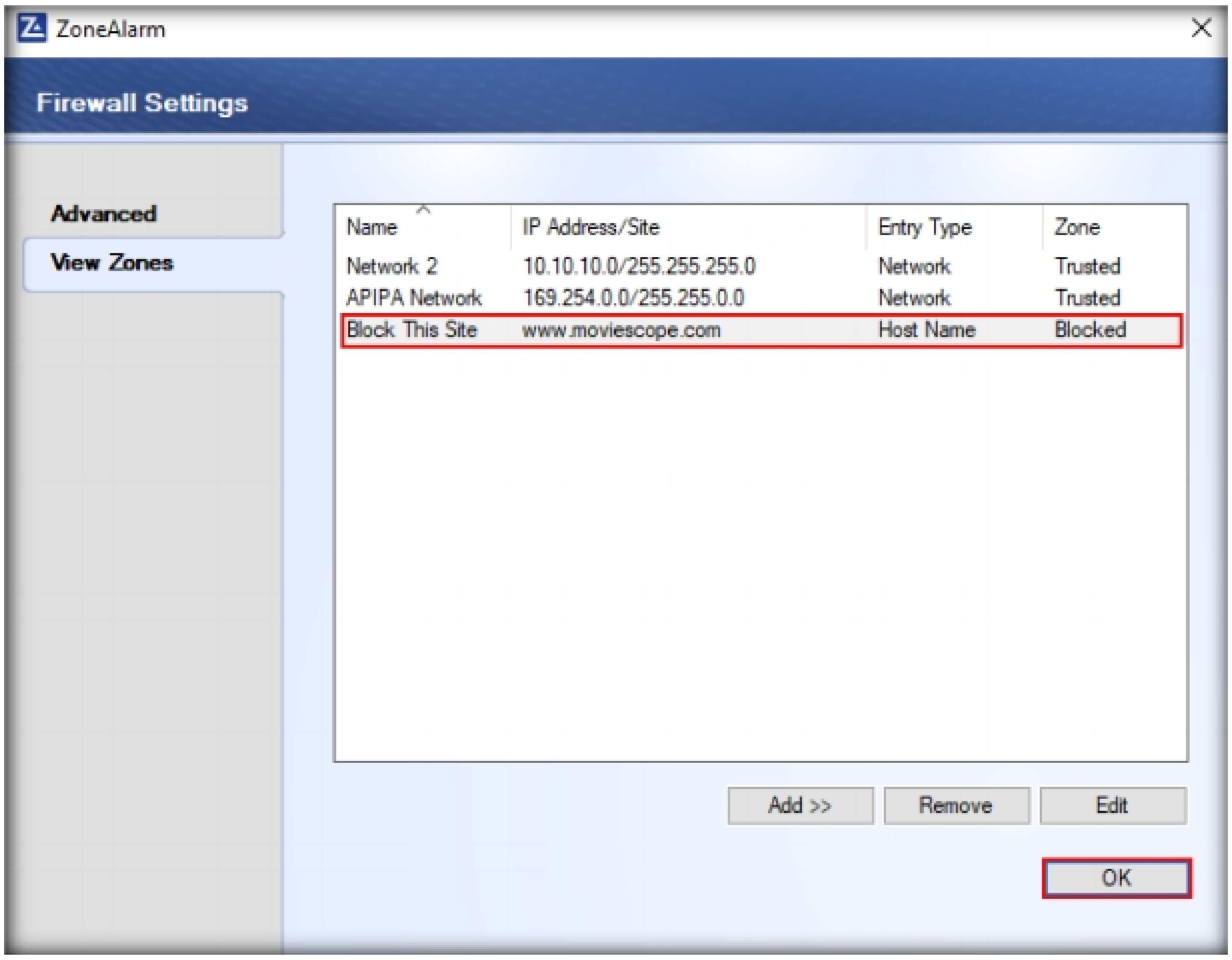


Add Host/Site to your Trusted or Blocked Zone by completing the fields below Name the Host/Site for easy reference later so you always know who you're trusting and who you're not.

Zone: Blocked
Host name: www.moviescope.com
Description: Block This Site
10.10.10.19

Figure 1.2.12: ZoneAlarm Adding Zone

23. The newly added rule appears in the **View Zones** section, as shown in the screenshot; click **OK**.

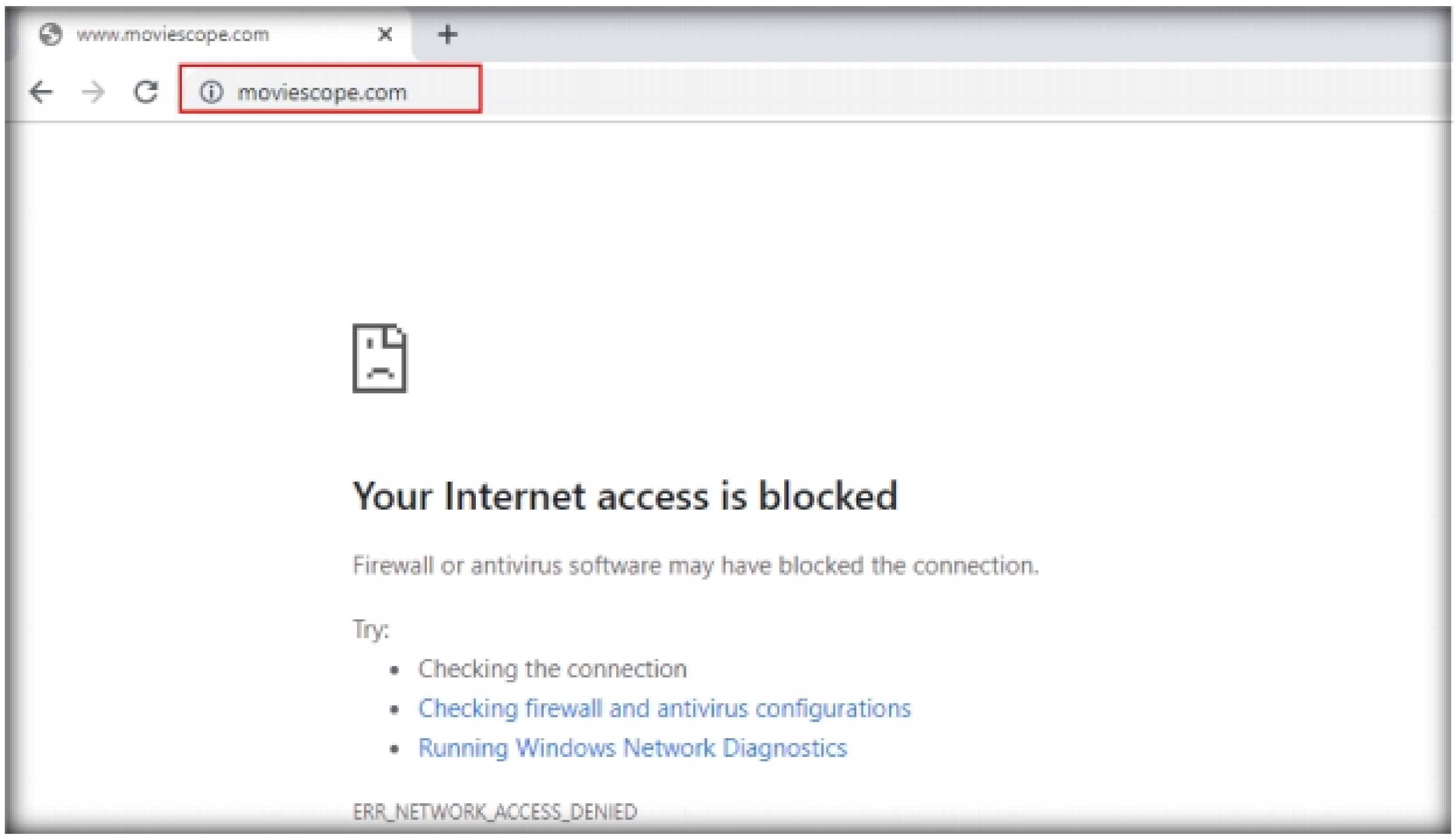


Name	IP Address/Site	Entry Type	Zone
Network 2	10.10.10.0/255.255.255.0	Network	Trusted
APIPA Network	169.254.0.0/255.255.0.0	Network	Trusted
Block This Site	www.moviescope.com	Host Name	Blocked

Figure 1.2.13: ZoneAlarm newly created rule

24. Open any browser (here, **Google Chrome**) and now try to browse the blocked website, that is, www.moviescope.com.

25. As you have created a rule in ZoneAlarm Firewall to block **www.moviescope.com** from browsing, you will receive a message as **Your Internet access is blocked**.



Your Internet access is blocked

Firewall or antivirus software may have blocked the connection.

Try:

- Checking the connection
- Checking firewall and antivirus configurations
- Running Windows Network Diagnostics

ERR_NETWORK_ACCESS_DENIED

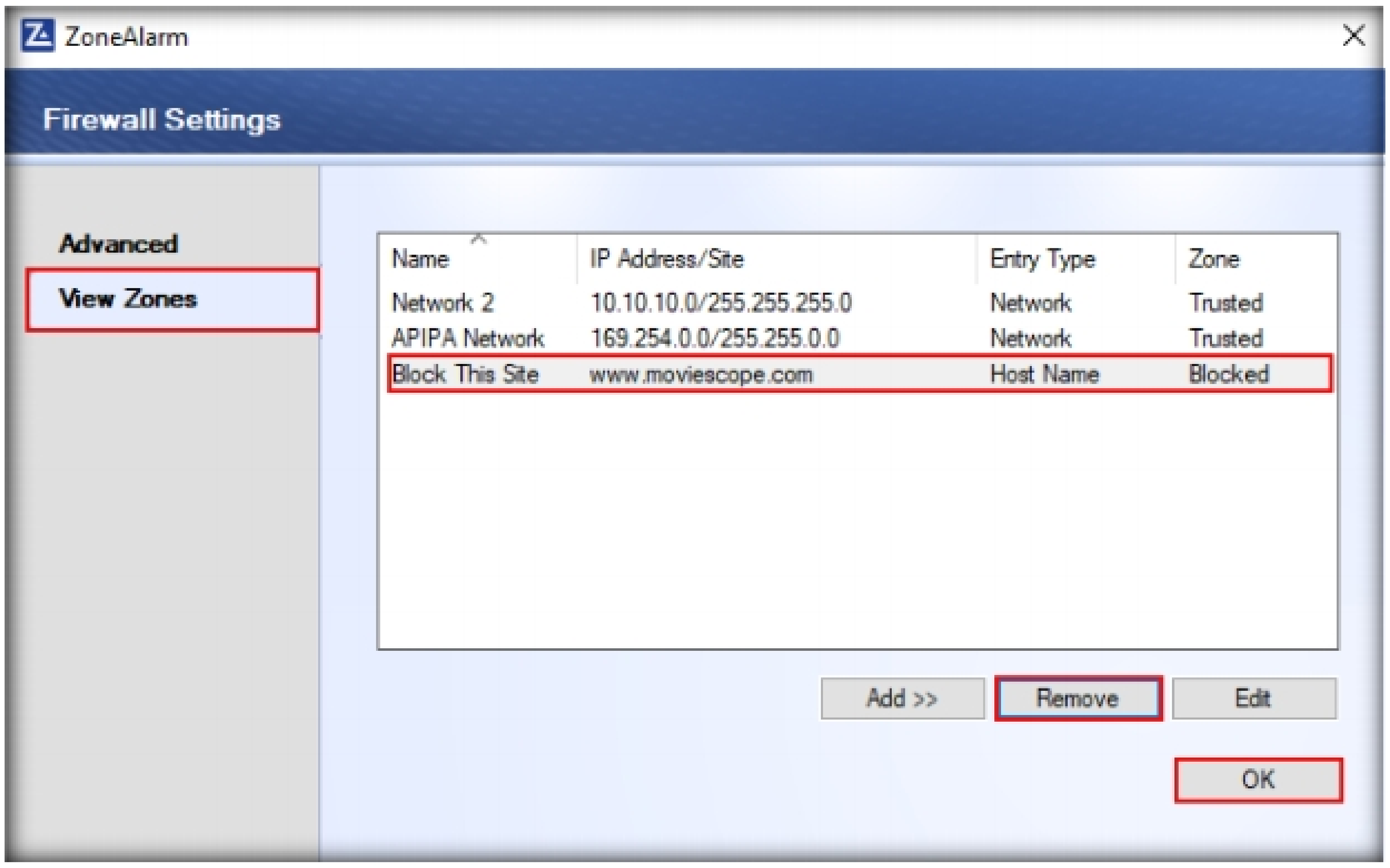
Figure 1.2.14: www.moviescope.com site blocked

Note: This is how you can block access for unwanted sites from browsing.

26. Before proceeding for the next task, go to the **ZoneAlarm Firewall Settings** window, select the newly created rule in the **View Zones** section, click **Remove**, and click **OK**.

Note: If a **Delete Confirmation** pop-up appears, click **Yes**.

27. This will remove the block access for the **www.moviescope.com** site.



Name	IP Address/Site	Entry Type	Zone
Network 2	10.10.10.0/255.255.255.0	Network	Trusted
APIPA Network	169.254.0.0/255.255.0.0	Network	Trusted
Block This Site	www.moviescope.com	Host Name	Blocked

Figure 1.2.15: ZoneAlarm removing www.moviescope.com from block list

28. Close the ZoneAlarm main window.

29. Click **Show hidden icon** (^) from the lower right section of **Desktop**. Right-click the **ZoneAlarm** icon and click **Exit** from the context menu.

Note: If a **Shut down** pop-up appears, click **Yes**.

30. Restart the **Windows 10** virtual machine.

31. After the system reboots, log in with the credentials **Admin** and **Pa$$w0rd**.

32. **Uninstall** ZoneAlarm in the **Windows 10** machine. To do so, launch **Control Panel → Programs and Features**. In the **Programs and Features** window, choose **ZoneAlarm Free Firewall** and click **Uninstall**. Follow the wizard-driven uninstallation process to remove ZoneAlarm from the **Windows 10** machine.

33. After the uninstallation is completed, you will receive a prompt to restart the machine; click **Yes** to restart.

34. Once the system reboots, turn off the **Windows Defender Firewall**.

    a. In the **Windows Defender Firewall** window, click the **Turn Windows Defender Firewall on or off** link in the left pane of the window

b. In the **Customise Settings** window, select the **Turn off Windows Defender Firewall (not recommended)** radio button for all Domain, Private and Public network settings, and then click **OK**

c. Again, in the **Windows Defender Firewall** window, click **Advanced settings** link in the left pane

d. Once the **Windows Defender Firewall with Advanced Security** appears on the screen, click the **Windows Defender Firewall Properties** link in the **Overview** section

e. The **Windows Defender Firewall with Advanced Security on Local Computer Properties** window appears; in the **Domain Profile** tab, choose **Off** from the **Firewall state** drop-down list. Then, navigate to the **Private Profile** and **Public Profile** tabs and ensure that the **Firewall state** is **Off**. Click **Apply**, and then click **OK**

You can also use other firewalls such as **ManageEngine Firewall Analyzer** (https://www.manageengine.com), **pfSense** (https://www.pfsense.org), **Sophos XG Firewall** (https://www.sophos.com), and **Comodo Firewall** (https://personalfirewall.comodo.com) to block access to a particular website or IP address.

35. Close all open windows.

36. Turn off the **Windows Server 2019** virtual machine.

TASK 3

Detect Malicious Network Traffic using HoneyBOT

Here, we will use the HoneyBOT tool to detect malicious network traffic.

Note: Ensure that the **Windows 10** virtual machine is running.

1. Turn on the **Windows Server 2016** and **Parrot Security** virtual machines.

2. In the **Windows Server 2016** virtual machine, log in with the credentials **Administrator** and **Pa$$w0rd**.

3. Navigate to **Z:\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots\Honeypot Tools\HoneyBOT**. Double-click **HoneyBOT_018.exe** to launch the HoneyBOT installer. Follow the wizard-driven steps to install HoneyBOT.

HoneyBOT is a medium interaction honeypot for windows. A honeypot creates a safe environment to capture and interact with unsolicited traffic on a network. HoneyBOT is an easy-to-use solution that is ideal for network security research or as part of an early-warning IDS.

Note: If the **User Account Control** window appears, click **Yes**.

4. Once the installation of HoneyBOT completes, in the **Completing the HoneyBot Setup Wizard** window, uncheck the **Launch HoneyBOT** option, click **Finish**.

5. Now, click the **Start** icon from the left-bottom of **Desktop**. Under **Recently added** applications, right-click **HoneyBOT → More → Run as administrator**, as shown in the screenshot.

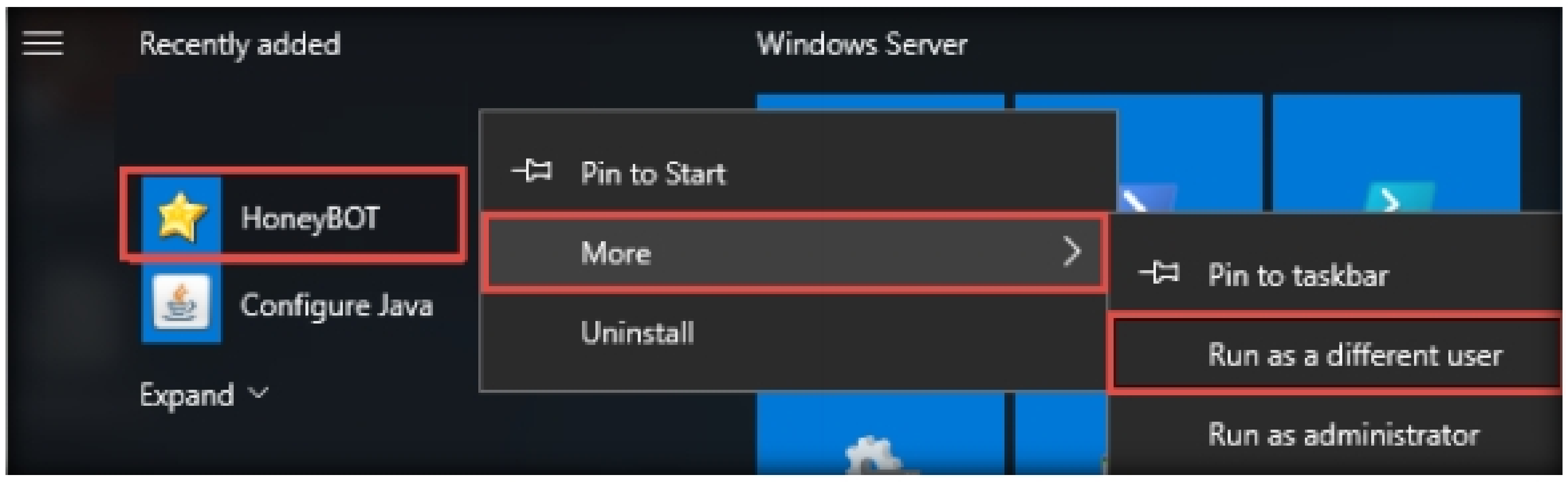


Figure 1.3.1: Launch HoneyBOT

6. The **HoneyBOT** configuration pop-up appears; click **Yes** to configure HoneyBOT.

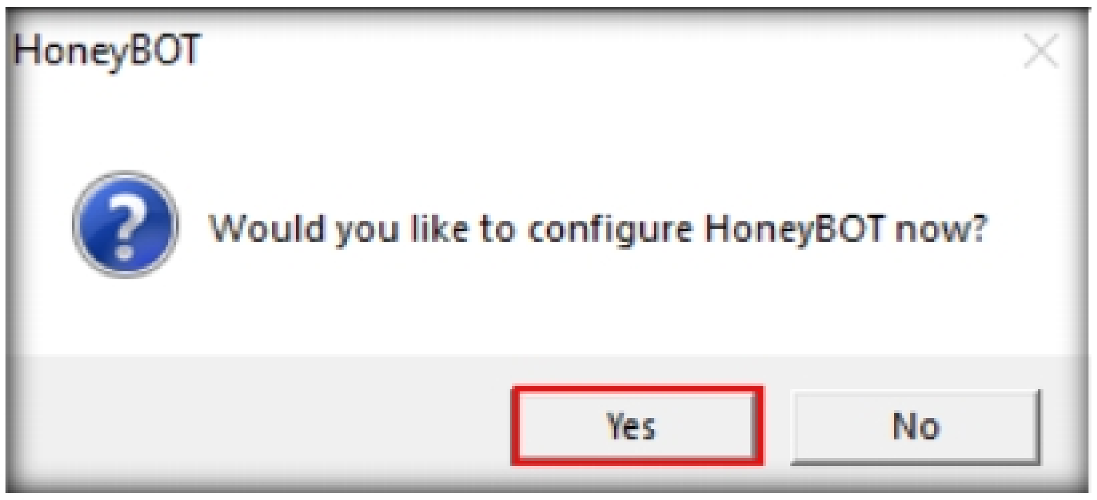
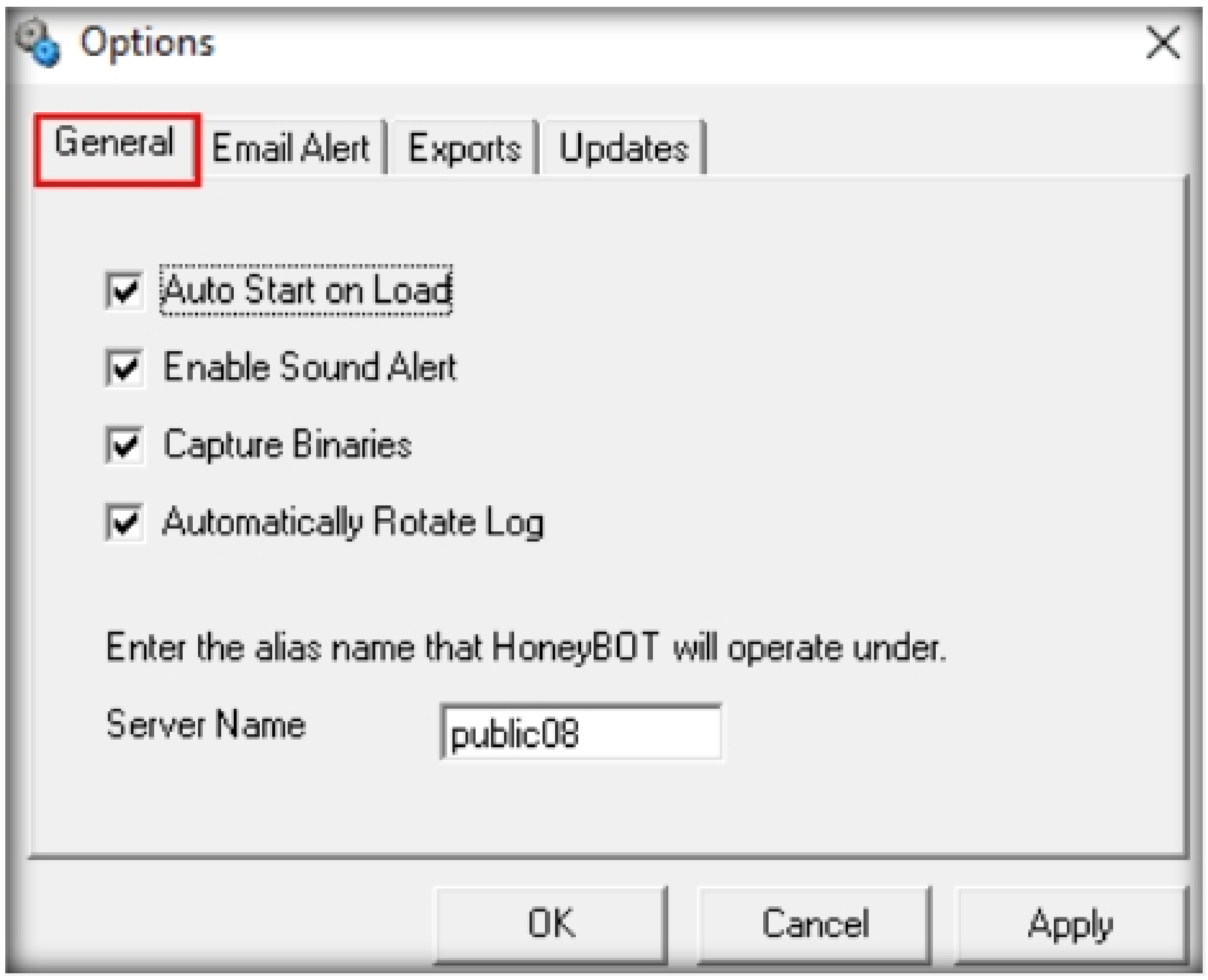

HoneyBOT
Would you like to configure HoneyBOT now?
Yes
No

Figure 1.3.2: HoneyBOT configuration pop-up

7. The HoneyBOT **Options** window appears with default options checked on the **General** settings tab. Leave the default settings or modify them accordingly.

8. In this task, we are leaving the settings on default for the **General** tab in the **Options** window.


Options
General
Email Alert
Exports
Updates
OK
Cancel
Apply

☑ Auto Start on Load
☑ Enable Sound Alert
☑ Capture Binaries
☑ Automatically Rotate Log

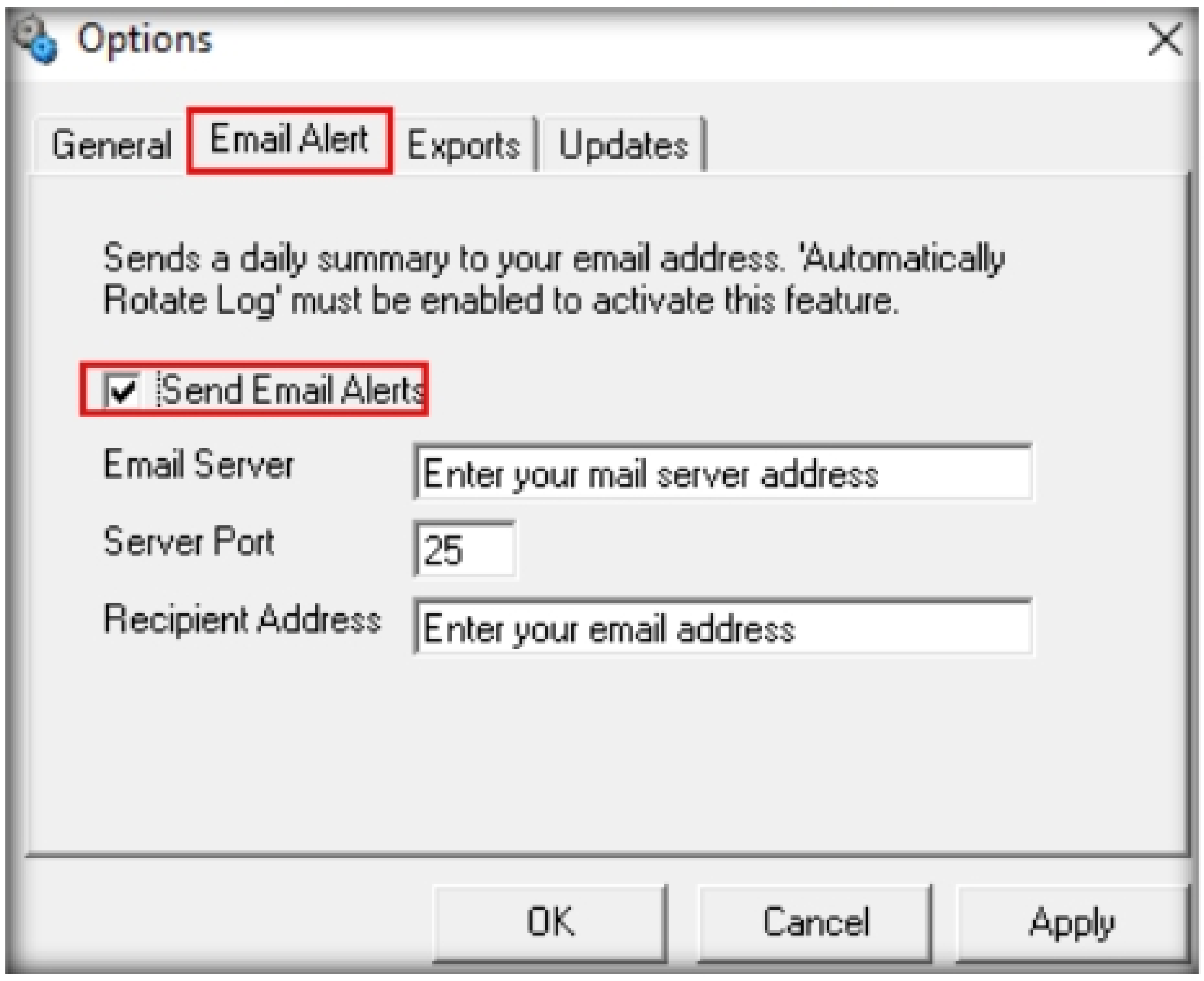
Enter the alias name that HoneyBOT will operate under.

Server Name: public08

Figure 1.3.3: HoneyBOT Options-General

9. Click the **Email Alert** tab; if you want HoneyBOT to send you email alerts, check **Send Email Alerts**, and fill in the respective fields.

   Note: In this task, we will not be providing any details for email alerts.



Sends a daily summary to your email address. 'Automatically Rotate Log' must be enabled to activate this feature.

☑ Send Email Alerts

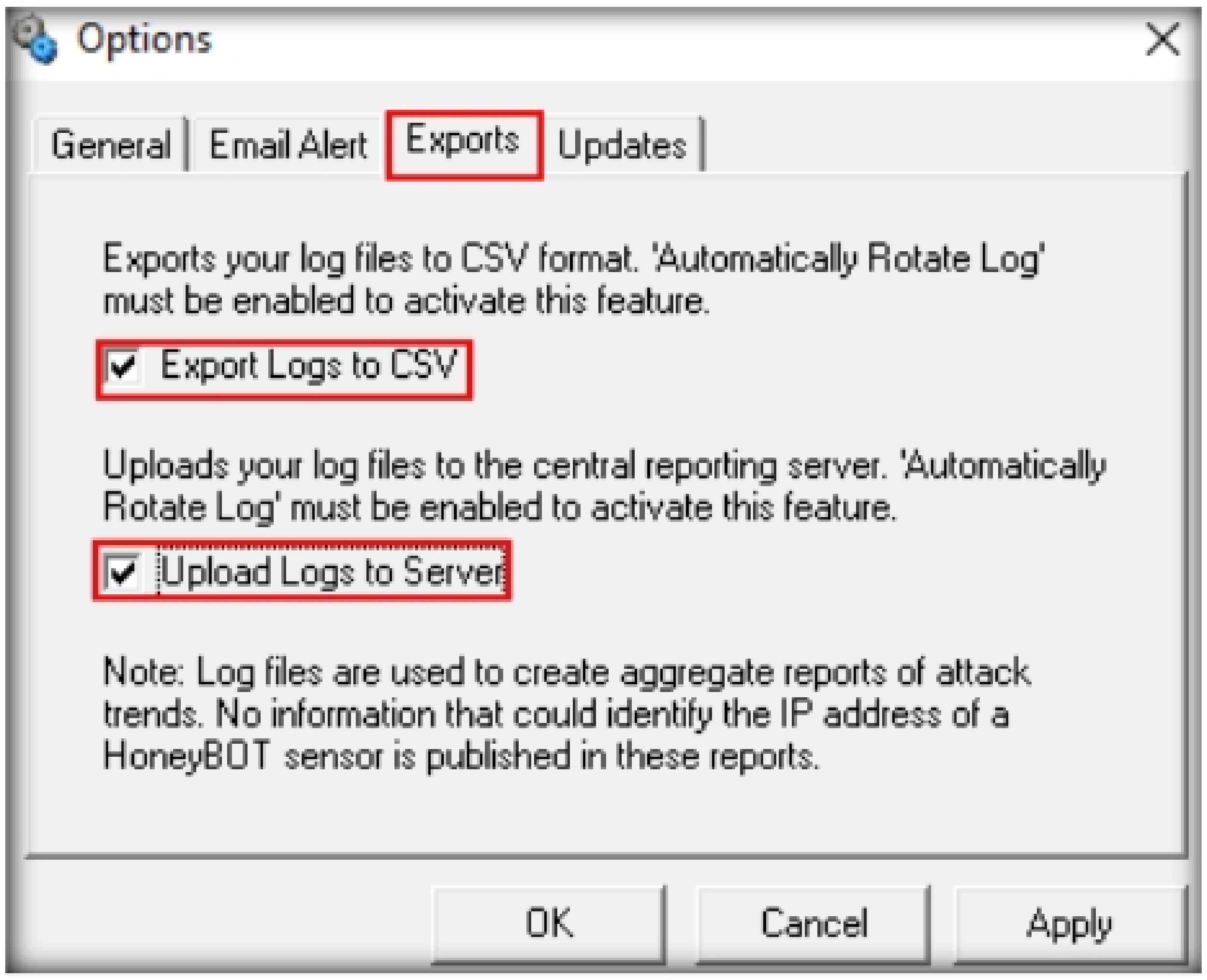
Email Server: Enter your mail server address

Server Port: 25

Recipient Address: Enter your email address

Figure 1.3.4: HoneyBOT Options-Email Alert

10. On the **Exports** tab, in which you can export the logs recorded by HoneyBOT, choose the required option to view the reports, and then proceed to the next step.



Exports your log files to CSV format. 'Automatically Rotate Log' must be enabled to activate this feature.

☑ Export Logs to CSV

Uploads your log files to the central reporting server. 'Automatically Rotate Log' must be enabled to activate this feature.

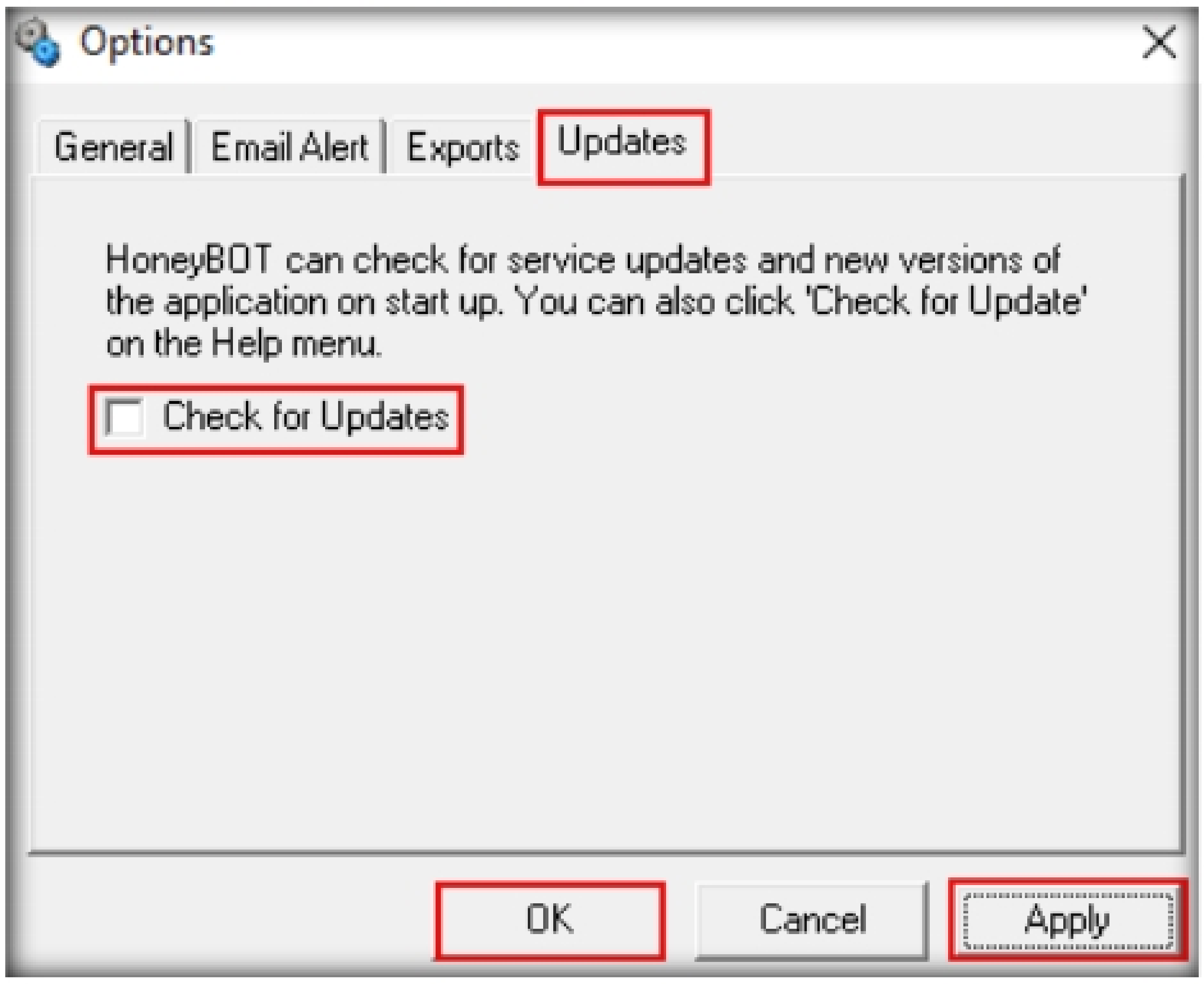
☑ Upload Logs to Server

Note: Log files are used to create aggregate reports of attack trends. No information that could identify the IP address of a HoneyBOT sensor is published in these reports.

Figure 1.3.5: HoneyBOT Options-Exports

11. On the **Updates** tab, uncheck **Check for Updates**; click **Apply** and click **OK** to continue.

Note: If a **Bindings** pop-up appears, click **OK** to continue.


Options
General
Email Alert
Exports
Updates
OK
Cancel
Apply

HoneyBOT can check for service updates and new versions of the application on start up. You can also click 'Check for Update' on the Help menu.

☐ Check for Updates

Figure 1.3.6: HoneyBOT Options-Updates

12. The **HoneyBOT** main window appears, as shown in the screenshot.
13. Now, leave the HoneyBOT window running on **Windows Server 2016**.

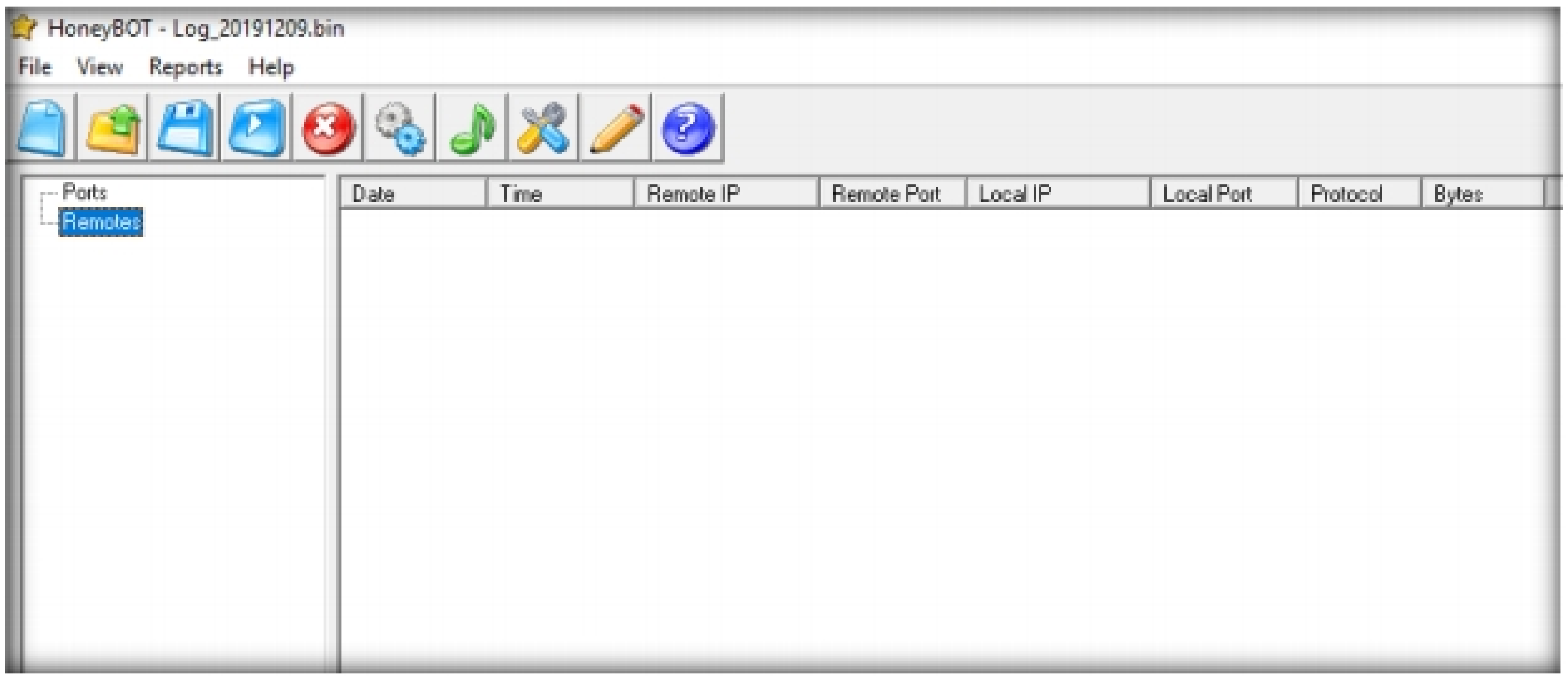

HoneyBOT - Log_20191209.bin
File
View
Reports
Help
Ports
Remotes
Date
Time
Remote IP
Remote Port
Local IP
Local Port
Protocol
Bytes

Figure 1.3.7: HoneyBOT main window

14. Switch to the **Parrot Security** virtual machine.
15. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

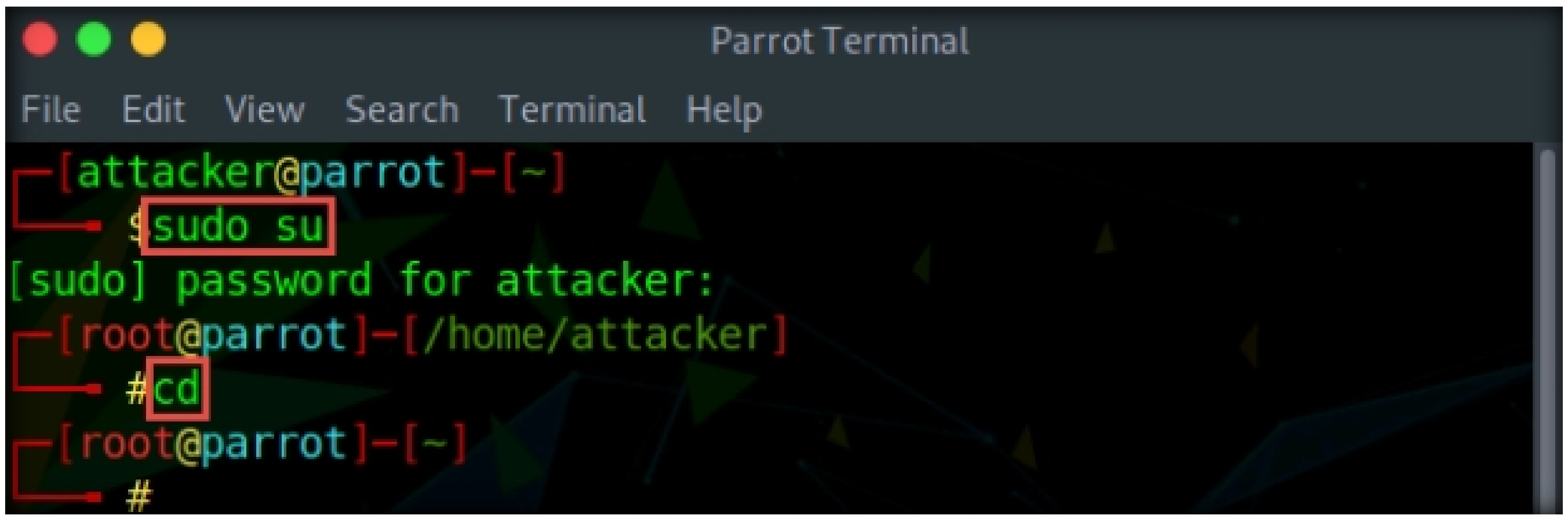
- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

16. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
17. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
18. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

19. Now, type **cd** and press **Enter** to jump to the root directory.

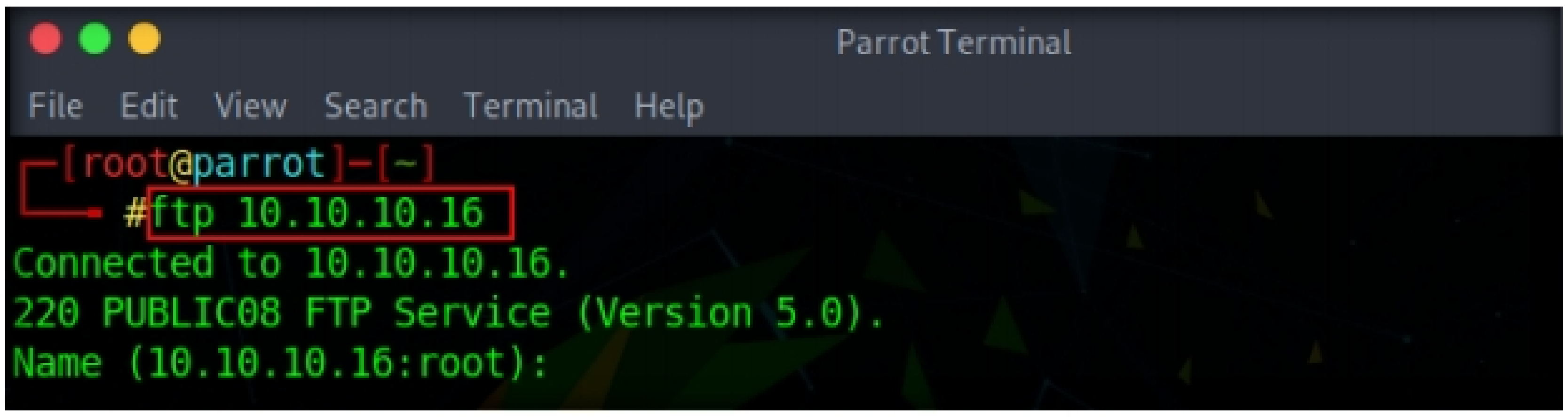


```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd
┌─[root@parrot]─[~]
└──╼ #
```

Figure 1.3.8: Running the programs as a root user

20. In the terminal window, type **ftp <IP Address of the Windows Server 2016 machine>** and press **Enter**.
21. You will be prompted for the ftp credentials of the **Windows Server 2016** machine.
22. In this task, the IP address of **Windows Server 2016** is **10.10.10.16**; this may differ in your lab environment.

Note: If Parrot Security sends an error message stating that the ftp command is not found, then install ftp with the "**apt-get install ftp**" command.



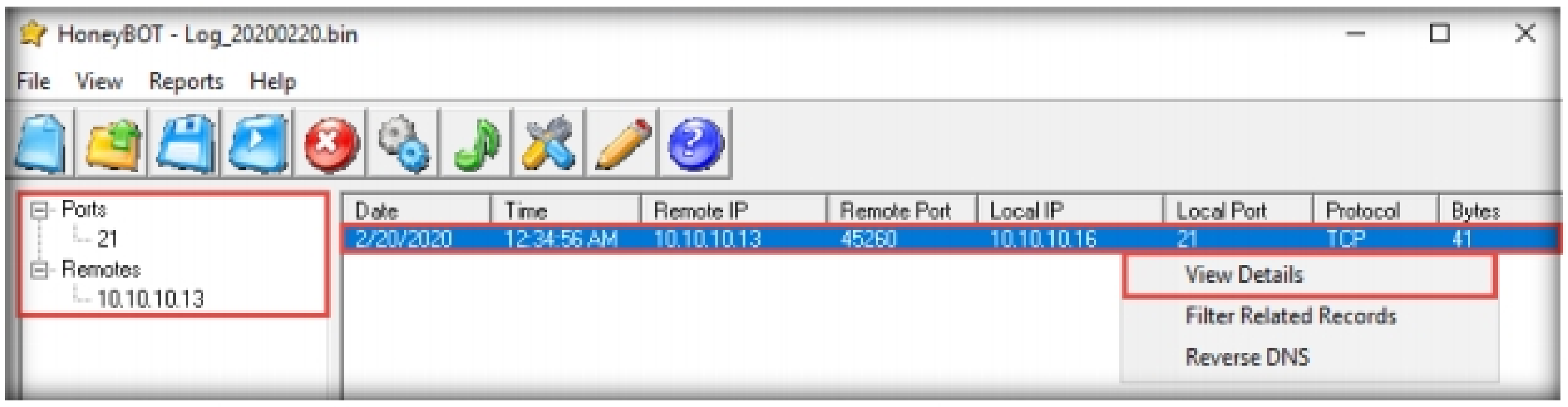
```
┌─[root@parrot]─[~]
└──╼ #ftp 10.10.10.16
Connected to 10.10.10.16.
220 PUBLIC08 FTP Service (Version 5.0).
Name (10.10.10.16:root):
```

Figure 1.3.9: Running ftp command in Parrot Security

23. Return to the **Windows Server 2016** virtual machine. In the **HoneyBOT** window, expand the **Ports** and **Remotes** node from the left-pane.
24. Under **Ports**, you can see the port numbers from which **Windows Server 2016** received requests or attacks.

25. Under **Remotes**, you can view the recorded IP addresses through which Windows Server 2016 received requests.

26. Now, right-click any IP address or Port on the left, and click **View Details**, as shown in the screenshot, to view the complete details of the request or attack recorded by HoneyBOT.


HoneyBOT - Log_20200220.bin
File
View
Reports
Help
Ports
21
Remotes
10.10.10.13
View Details
Filter Related Records
Reverse DNS

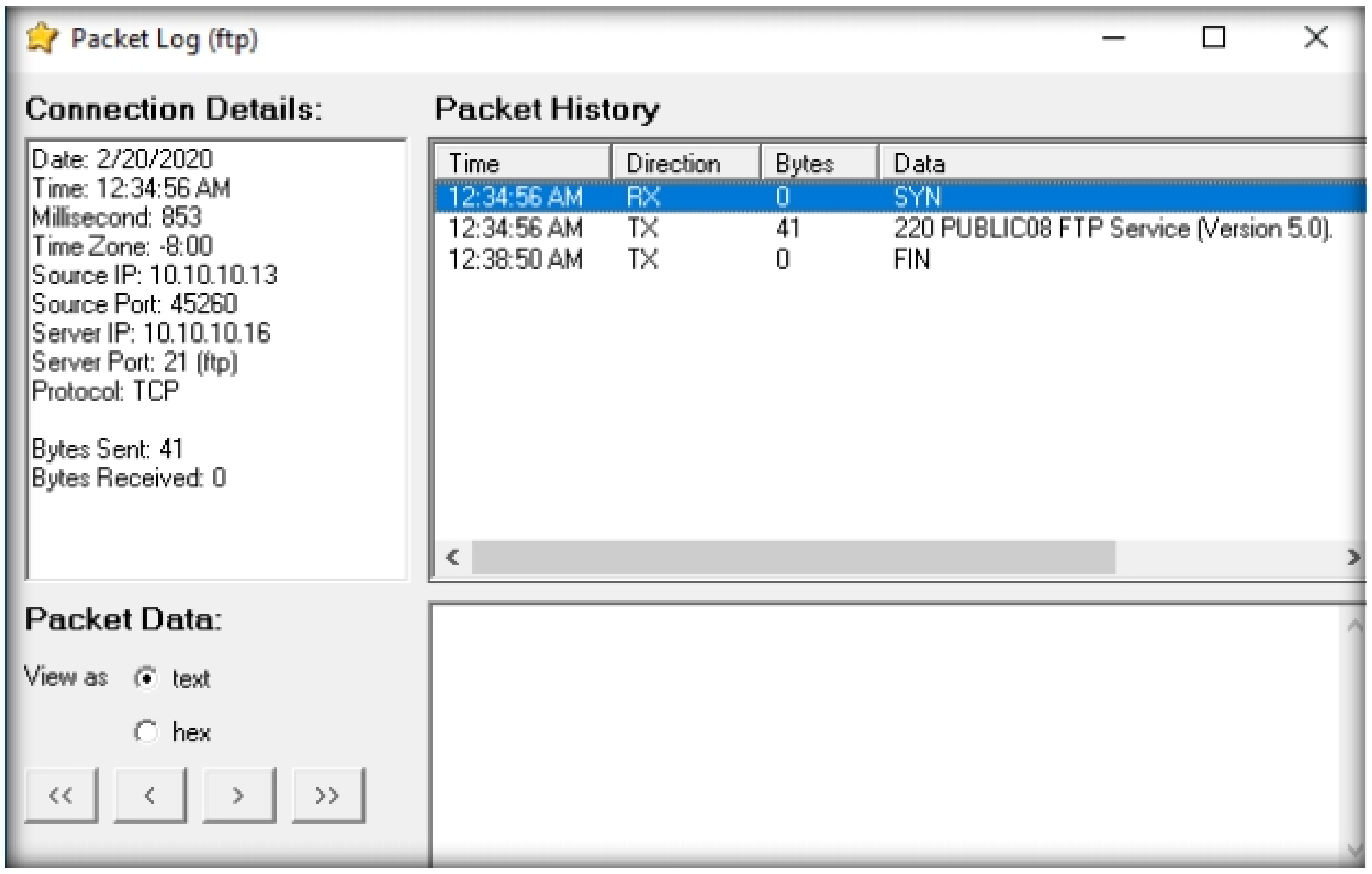
Date	Time	Remote IP	Remote Port	Local IP	Local Port	Protocol	Bytes
2/20/2020	12:34:56 AM	10.10.10.13	45260	10.10.10.16	21	TCP	41

Figure 1.3.10: HoneyBOT captured traffic

27. The **Packet Log** window appears, as shown in the screenshot. This displays the complete log details of the request captured by HoneyBOT.

28. In the screenshot, under **Connection Details**, you can view the Date and Time of the connection established as well as the protocol used.

29. **Connection Details** also shows the Source IP, Port, and Server Port, as shown below.


Packet Log (ftp)
Connection Details:
Packet History
Packet Data:
View as
● text
○ hex
<<
<
>
>>

Date: 2/20/2020
Time: 12:34:56 AM
Millisecond: 853
Time Zone: -8:00
Source IP: 10.10.10.13
Source Port: 45260
Server IP: 10.10.10.16
Server Port: 21 (ftp)
Protocol: TCP

Bytes Sent: 41
Bytes Received: 0

Time	Direction	Bytes	Data
12:34:56 AM	RX	0	SYN
12:34:56 AM	TX	41	220 PUBLIC08 FTP Service (Version 5.0).
12:38:50 AM	TX	0	FIN

Figure 1.3.11: HoneyBOT packet log information

30. Simultaneously, you can run the telnet command on the **Parrot Security** machine and observe the log recorded by **HoneyBOT** on **Windows Server 2016**.

31. Close all open windows in the **Windows Server 2016**, **Windows 10** and **Parrot Security**.

32. Turn off the **Parrot Security**, **Windows 10**, and **Windows Server 2019** virtual machines.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ **Yes**	☐ **No**
Platform Supported	
☑ **Classroom**	☑ **iLabs**

Lab
2

Evade Firewalls using Various Evasion Techniques

Bypassing a firewall is a technique where an attacker manipulates the attack sequence to avoid being detected by the underlying security firewall.

ICON KEY

- 📁 Valuable information
- ✎ Test your knowledge
- 💻 Web exercise
- 📖 Workbook review

Lab Scenario

Firewalls and IDSs are intended to prevent port scanning tools such as Nmap, from receiving a precise measure of significant data of the frameworks that they are scanning. However, these prevention measures can be easily overcome: Nmap has numerous features that were created specifically to bypass these protections. It has the ability to issue a mapping of a system framework, through which you can view a substantial amount of information, from OS renditions to open ports. Firewalls and interruption recognition frameworks are made to keep Nmap and other applications from obtaining that data.

As an ethical hacker or penetration tester, you will come across systems behind firewalls that prevent you from attaining the information that you need. Therefore, you will need to know how to avoid the firewall rules and to glean information about a host. This step in a penetration test is called Firewall Evasion Rules.

Lab Objectives

- Bypass windows firewall using Nmap evasion techniques
- Bypass firewall rules using HTTP/FTP tunneling

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2016 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine

- Web browsers with an Internet connection
- Administrator privileges to run the tools
- HTTHost located at **E:\CEH-Tools\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots\HTTP Tunneling Tools\HTTHost**
- HTTPort located at **E:\CEH-Tools\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots\HTTP Tunneling Tools\HTTPort**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest version, the screenshots shown in the lab might differ.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots

Lab Duration

Time: 30 Minutes

Overview of Firewalls Evasion Techniques

A firewall operates on a predefined set of rules. Using extensive knowledge and skill, an attacker can bypass the firewall by employing various bypassing techniques. Using these techniques, the attacker tricks the firewall to not filter the malicious traffic that he/she generates.

The following are some firewall bypassing techniques:

- Port Scanning
- Firewalking
- Banner Grabbing
- IP Address Spoofing
- Source Routing
- Tiny Fragments
- Using an IP Address in Place of URL
- Using Anonymous Website Surfing Sites
- Using a Proxy Server
- ICMP Tunneling
- ACK Tunneling
- HTTP Tunneling
- SSH Tunneling
- DNS Tunneling
- Through External Systems
- Through MITM Attack
- Through Content
- Through XSS Attack

Lab Tasks

TASK 1

Bypass Windows Firewall using Nmap Evasion Techniques

Network/security administrators play a crucial role in creating security defenses within an organization. Though such defenses protect the machines in the network, there might still be an insider who may try to apply different evasion techniques to identify the services running on the target.

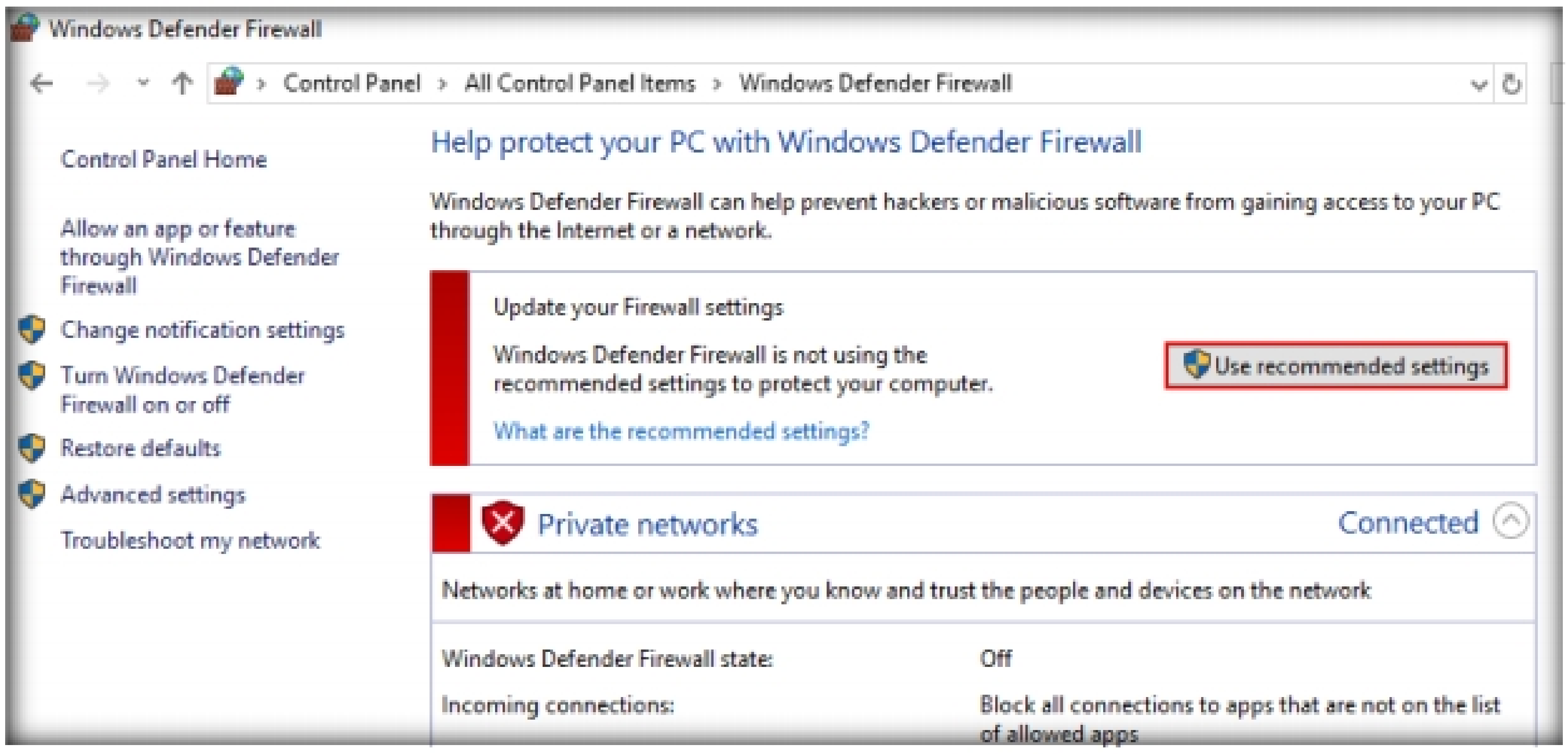
In this scenario, consider an admin has written certain Windows Firewall rules to block your system from reaching one of the machines in the network. You will be taught to use Nmap in such a way that you can perform recon on the target using other active machines on the network and identify the services running on the machine along with their open ports.

1. Before beginning this lab, turn on the **Windows 10**, **Windows Server 2019**, and **Parrot Security** virtual machines.

TASK 1.1

Turn On Windows Firewall

2. In the **Windows 10** machine, log in with the credentials **Admin** and **Pa$$w0rd**.
3. Open the **Control Panel**; navigate to **System and Security → Windows Defender Firewall** and click **Use recommended settings** to turn on Firewall.


Windows Defender Firewall
Control Panel › All Control Panel Items › Windows Defender Firewall
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
Use recommended settings
What are the recommended settings?
Private networks
Connected

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Update your Firewall settings

Windows Defender Firewall is not using the recommended settings to protect your computer.

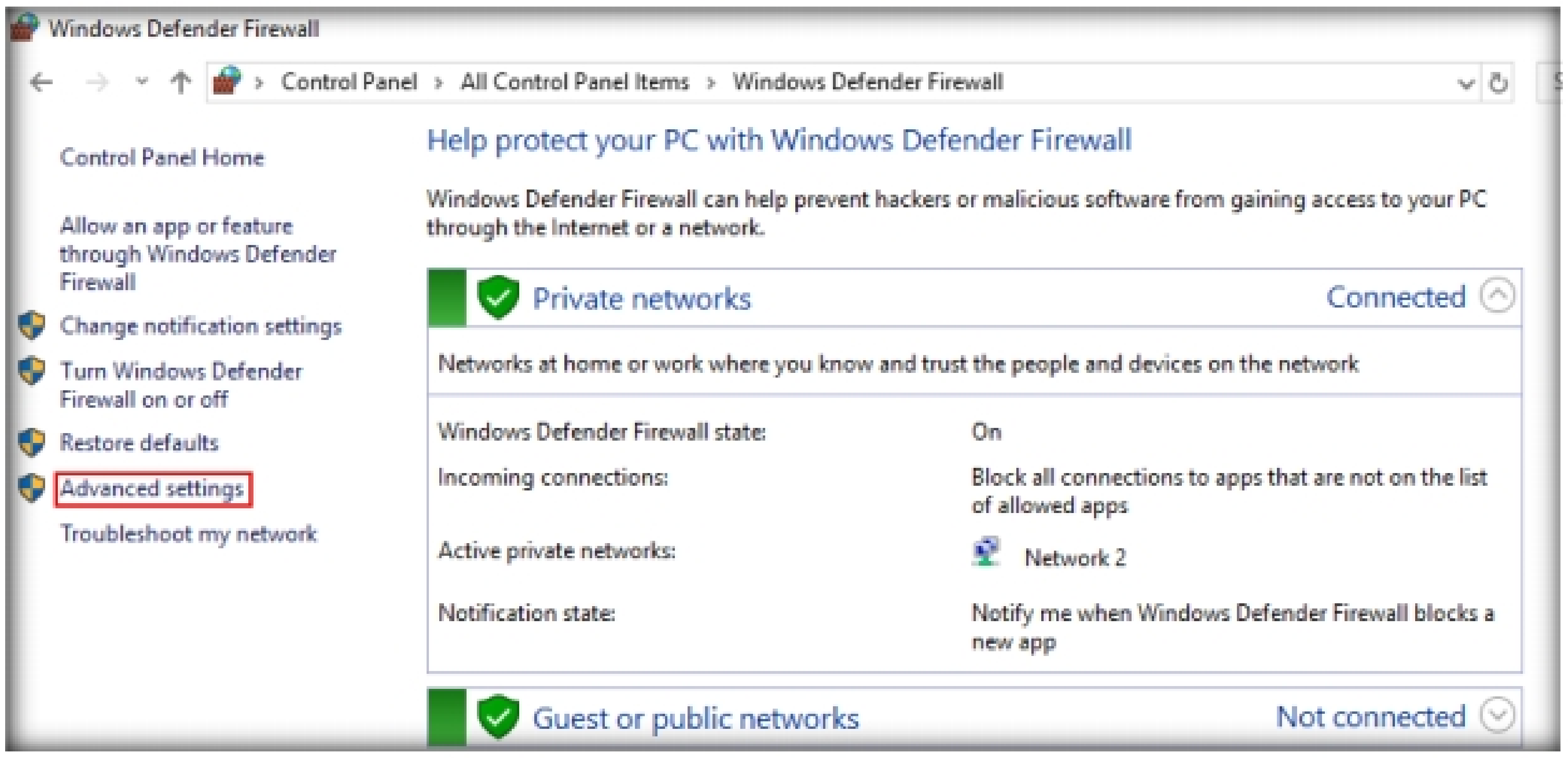
Networks at home or work where you know and trust the people and devices on the network

Windows Defender Firewall state: Off

Incoming connections: Block all connections to apps that are not on the list of allowed apps

Figure 2.1.1: Windows Defender Firewall

4. Now, you can see that the Firewall is enabled in the **Windows 10** machine. Click the **Advanced settings** link in the left pane.


Windows Defender Firewall
Control Panel › All Control Panel Items › Windows Defender Firewall
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
Private networks
Connected
Guest or public networks
Not connected

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Networks at home or work where you know and trust the people and devices on the network

Windows Defender Firewall state: On

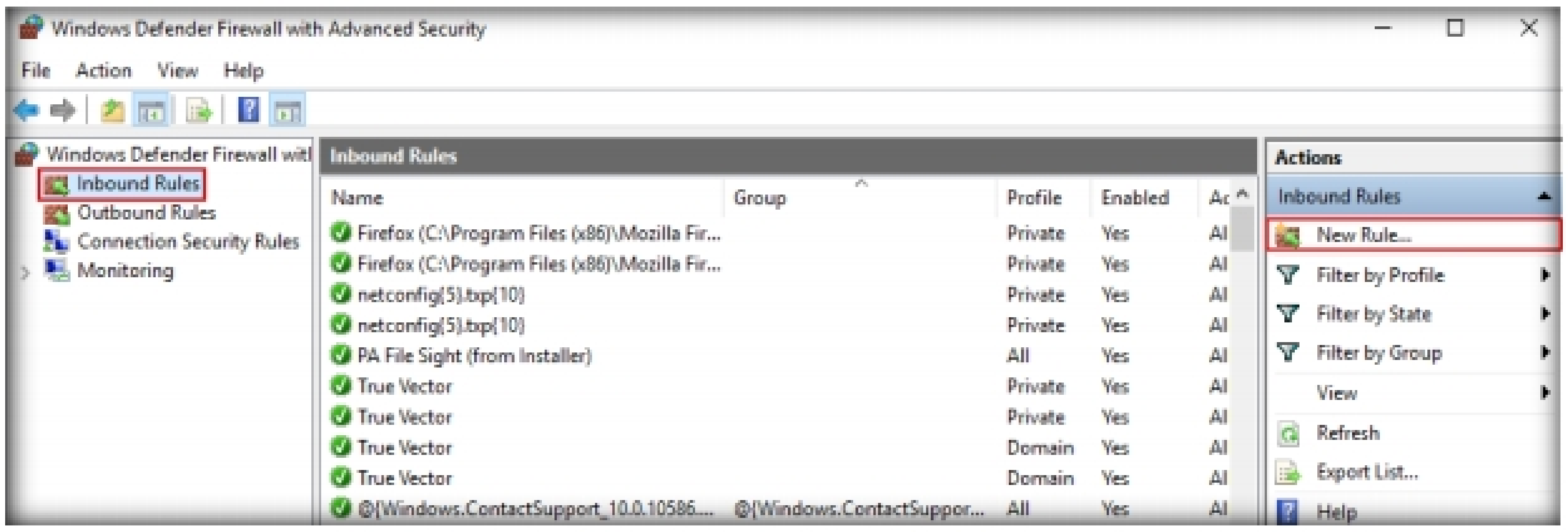
Incoming connections: Block all connections to apps that are not on the list of allowed apps

Active private networks: Network 2

Notification state: Notify me when Windows Defender Firewall blocks a new app

Figure 2.1.2: Windows Defender Firewall Turned On

5. The **Windows Defender Firewall with Advanced Security** window appears; here, we are going to create an inbound rule. Select **Inbound Rules** in the left pane and click **New Rule** under **Actions**.

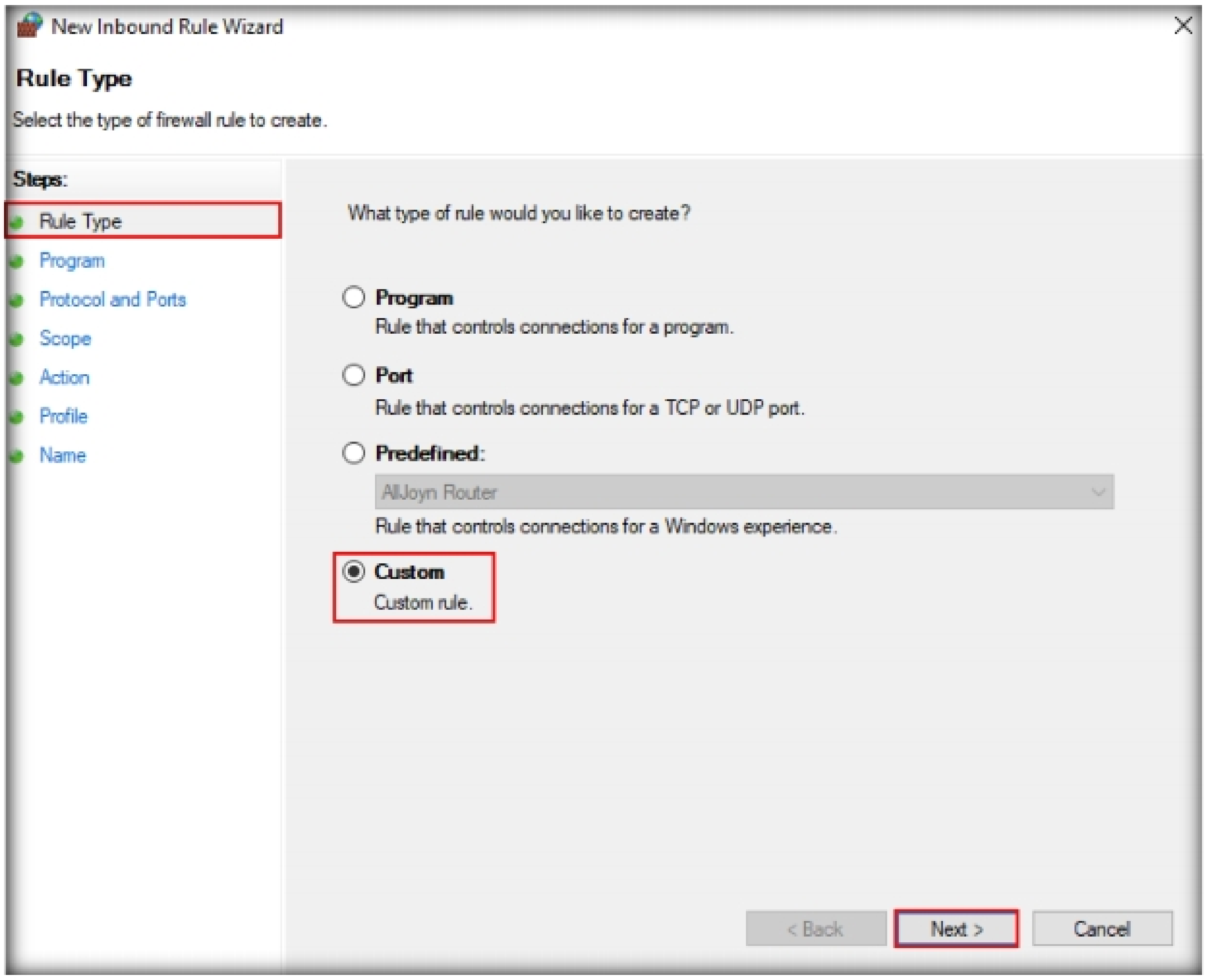

Windows Defender Firewall with Advanced Security
File
Action
View
Help
Windows Defender Firewall wit
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help

Inbound Rules

Name	Group	Profile	Enabled	Ac
Firefox (C:\Program Files (x86)\Mozilla Fir...		Private	Yes	Al
Firefox (C:\Program Files (x86)\Mozilla Fir...		Private	Yes	Al
netconfig(5).txp(10)		Private	Yes	Al
netconfig(5).txp(10)		Private	Yes	Al
PA File Sight (from Installer)		All	Yes	Al
True Vector		Private	Yes	Al
True Vector		Private	Yes	Al
True Vector		Domain	Yes	Al
True Vector		Domain	Yes	Al
@{Windows.ContactSupport_10.0.10586....	@{Windows.ContactSuppor...	All	Yes	Al

Figure 2.1.3: Creating Inbound Rule

6. The **New Inbound Rule Wizard** appears. In the **Rule Type** section, choose the **Custom** radio button to create a custom inbound rule and click **Next**.


New Inbound Rule Wizard
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
< Back
Next >
Cancel

Rule Type

Select the type of firewall rule to create.

What type of rule would you like to create?

○ **Program**
Rule that controls connections for a program.

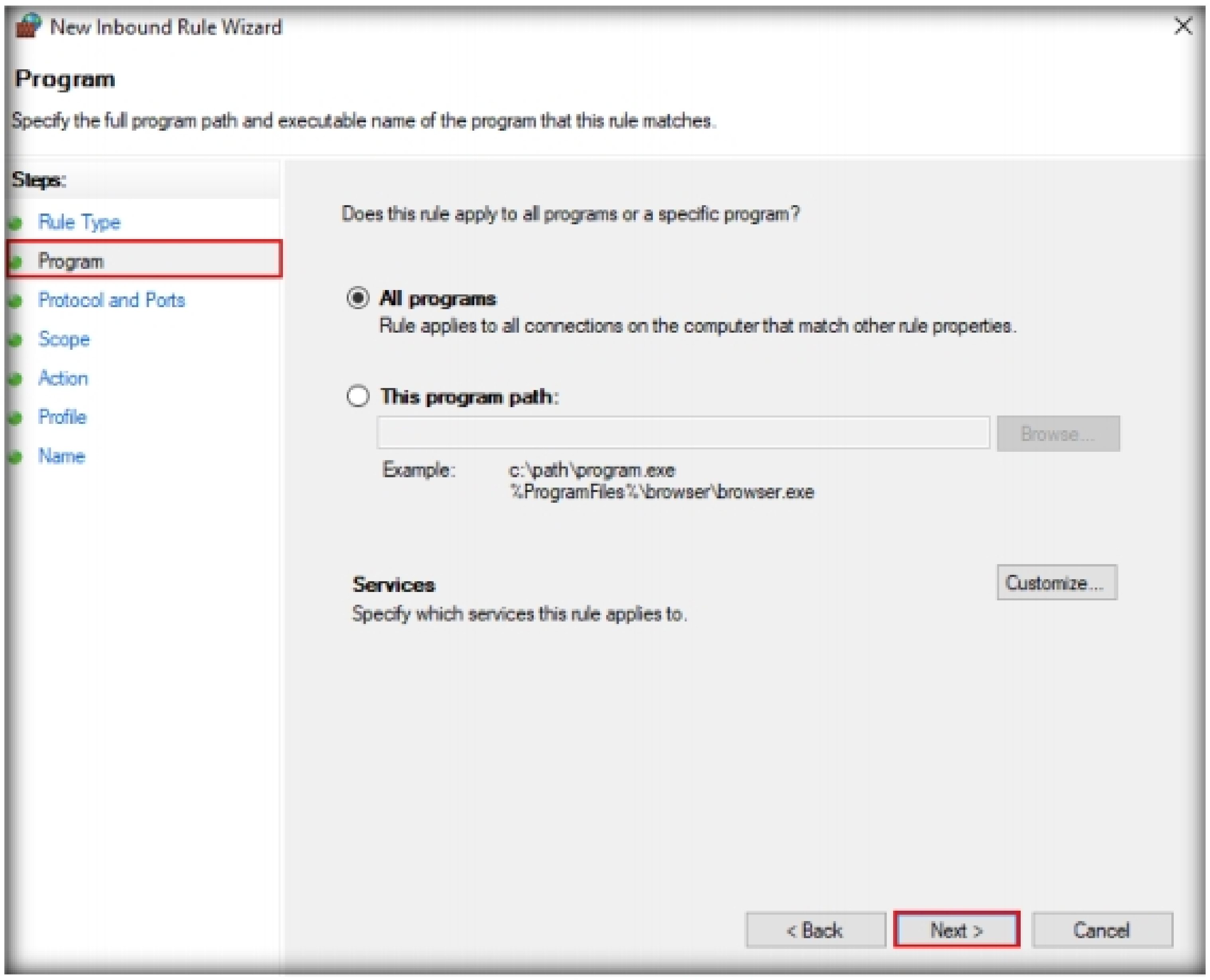
○ **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
AllJoyn Router
Rule that controls connections for a Windows experience.

● **Custom**
Custom rule.

Figure 2.1.4: Rule Type wizard

7. In the **Program** section, leave the settings to default and click **Next**.



New Inbound Rule Wizard

Program

Specify the full program path and executable name of the program that this rule matches.

Does this rule apply to all programs or a specific program?

● **All programs**
Rule applies to all connections on the computer that match other rule properties.

○ **This program path:**

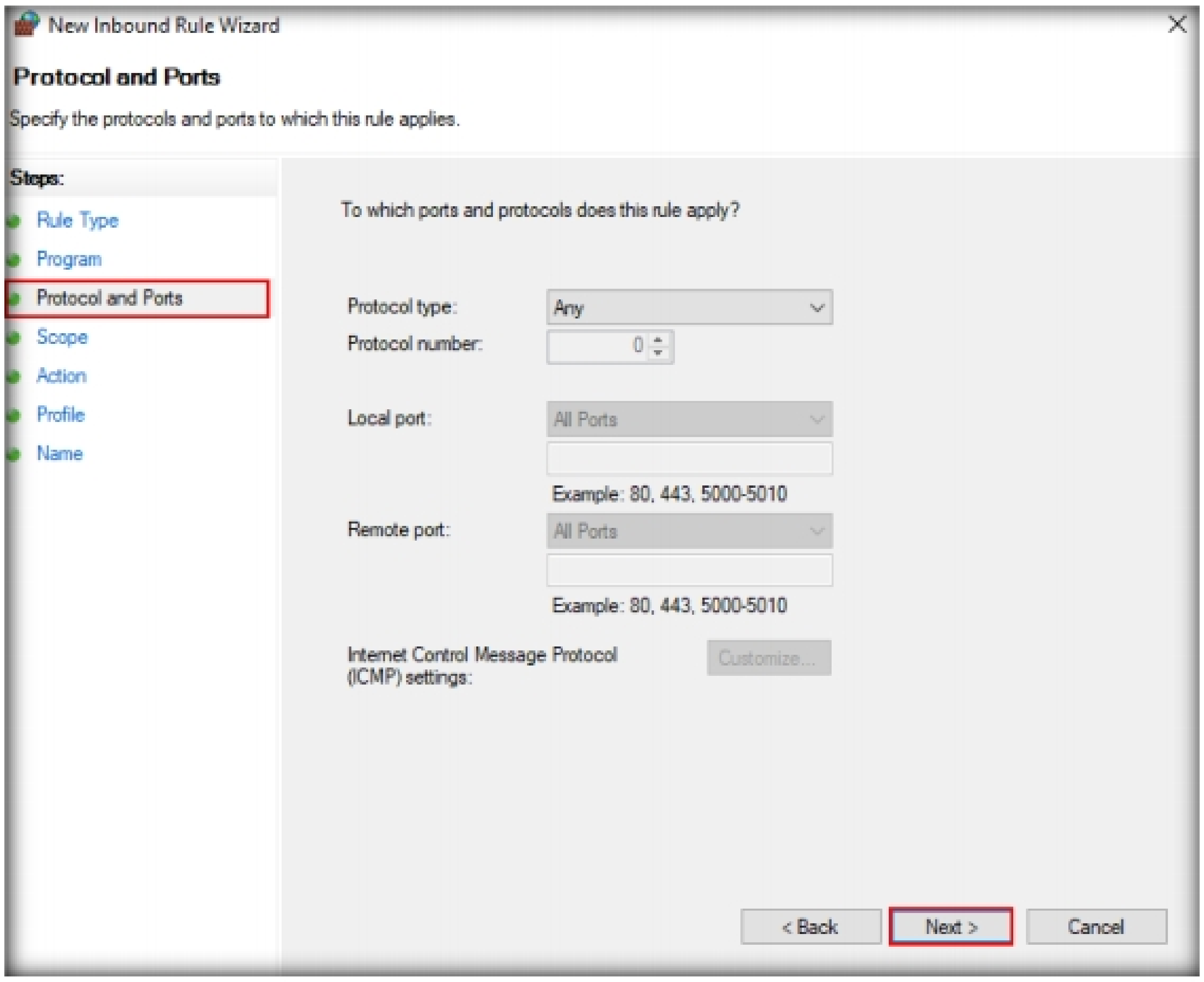
Example: c:\path\program.exe
%ProgramFiles%\browser\browser.exe

Services
Specify which services this rule applies to.

Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
Browse...
Customize...
< Back
Next >
Cancel

Figure 2.1.5: Program wizard

8. In the **Protocol and Ports** section, leave the settings to default and click **Next**.



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

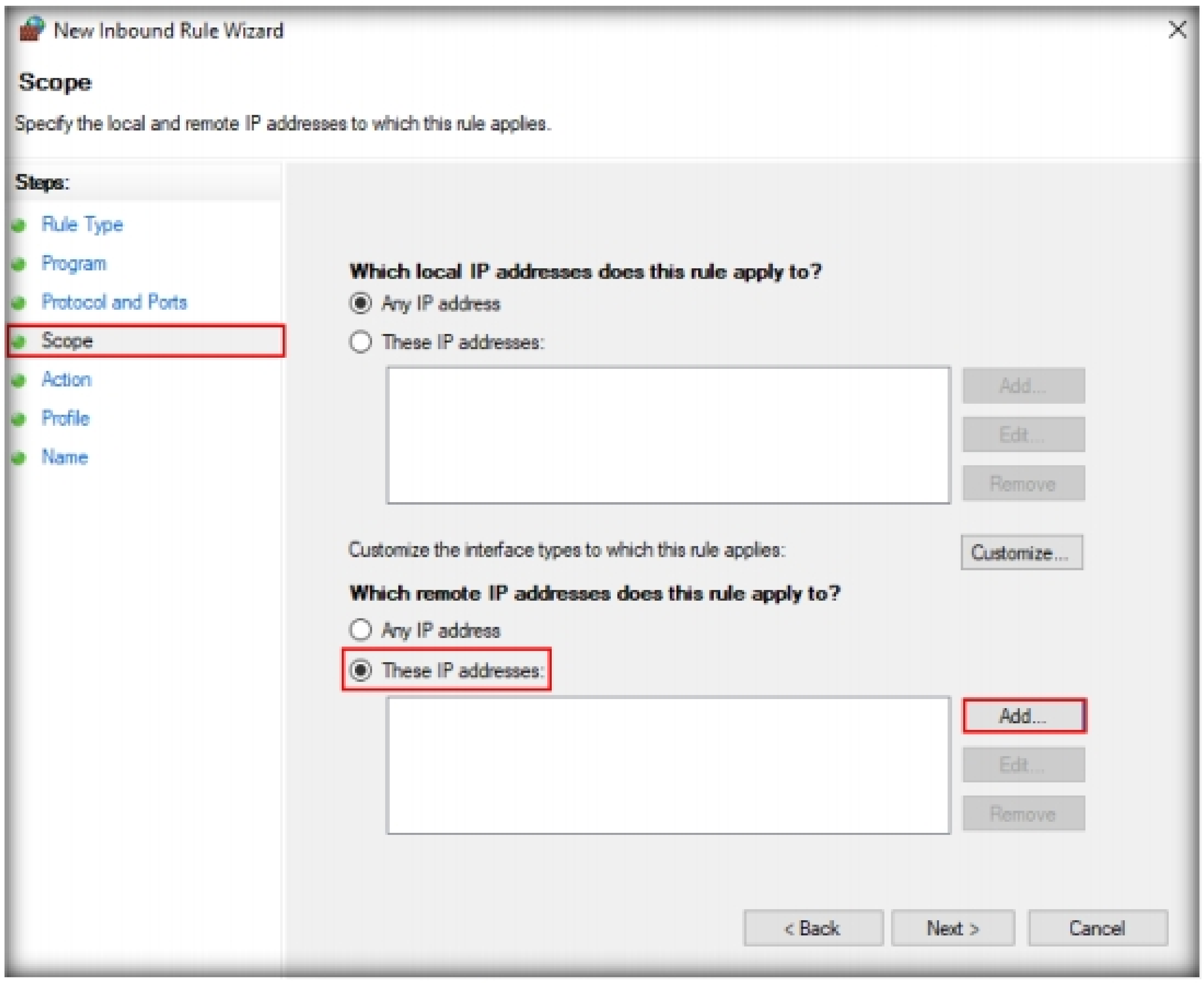
To which ports and protocols does this rule apply?

Protocol type: Any
Protocol number: 0
Local port: All Ports
Example: 80, 443, 5000-5010
Remote port: All Ports
Example: 80, 443, 5000-5010
Internet Control Message Protocol (ICMP) settings:

Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
Customize...
< Back
Next >
Cancel

Figure 2.1.6: Protocols and Ports wizard

9. In the **Scope** section, choose the **These IP addresses** radio button under **Which remote IP addresses does this rule apply to?**, and then click **Add**.

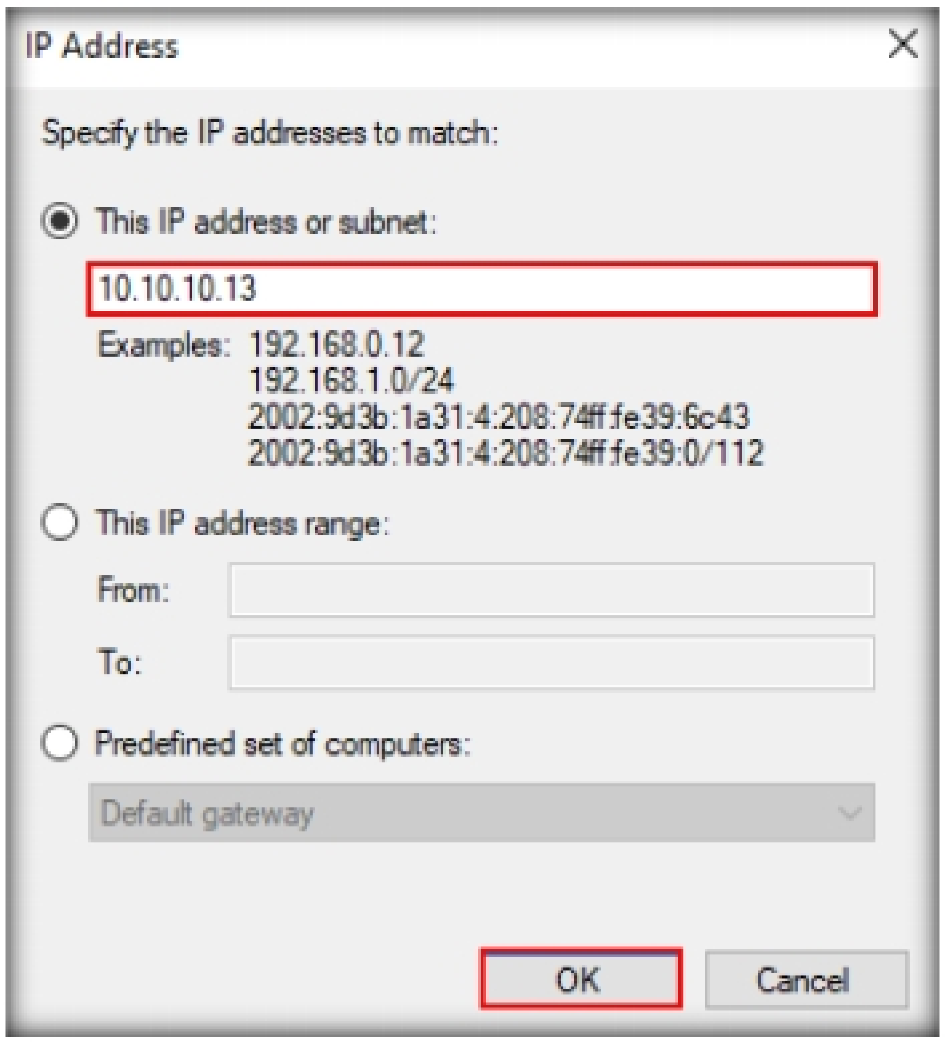


New Inbound Rule Wizard
Scope
Specify the local and remote IP addresses to which this rule applies.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
Which local IP addresses does this rule apply to?
Any IP address
These IP addresses:
Add...
Edit...
Remove
Customize the interface types to which this rule applies:
Customize...
Which remote IP addresses does this rule apply to?
Any IP address
These IP addresses:
Add...
Edit...
Remove
< Back
Next >
Cancel

Figure 2.1.7: Scope wizard

10. The **IP Address** pop-up appears; type the IP address of the **Parrot Security** virtual machine and click **OK**.

Note: In this task, the IP address of the Parrot Security is **10.10.10.13**, which may differ in your lab environment.

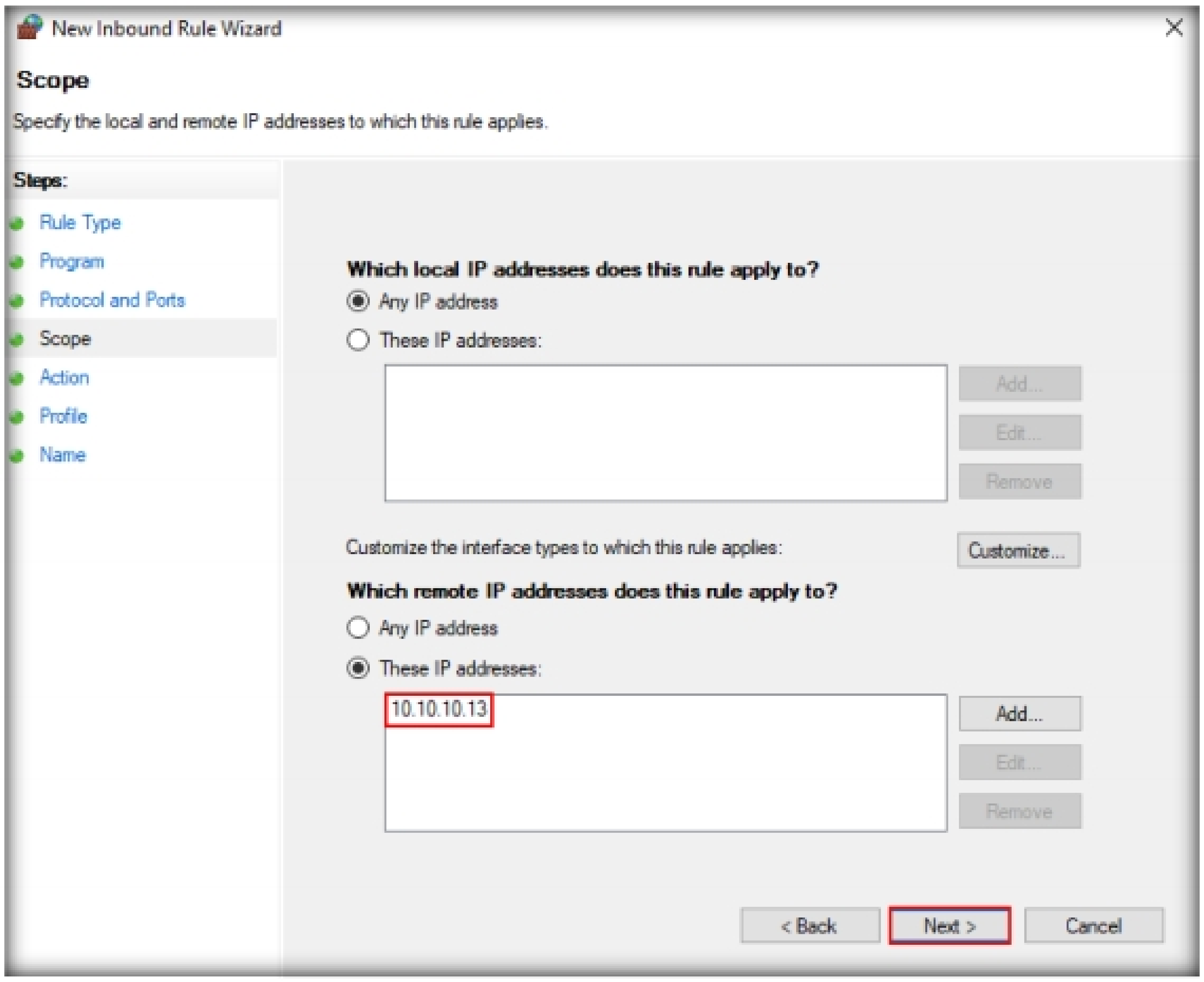


IP Address
Specify the IP addresses to match:
This IP address or subnet:
Examples: 192.168.0.12
192.168.1.0/24
2002:9d3b:1a31:4:208:74ff:fe39:6c43
2002:9d3b:1a31:4:208:74ff:fe39:0/112
This IP address range:
From:
To:
Predefined set of computers:
Default gateway
OK
Cancel

● This IP address or subnet: 10.10.10.13

Figure 2.1.8: IP Address window

11. Click **Next** in the **Scope** section once the IP address has been added.



New Inbound Rule Wizard

Scope

Specify the local and remote IP addresses to which this rule applies.

Which local IP addresses does this rule apply to?

● Any IP address

○ These IP addresses:

Customize the interface types to which this rule applies:

Which remote IP addresses does this rule apply to?

○ Any IP address

● These IP addresses:

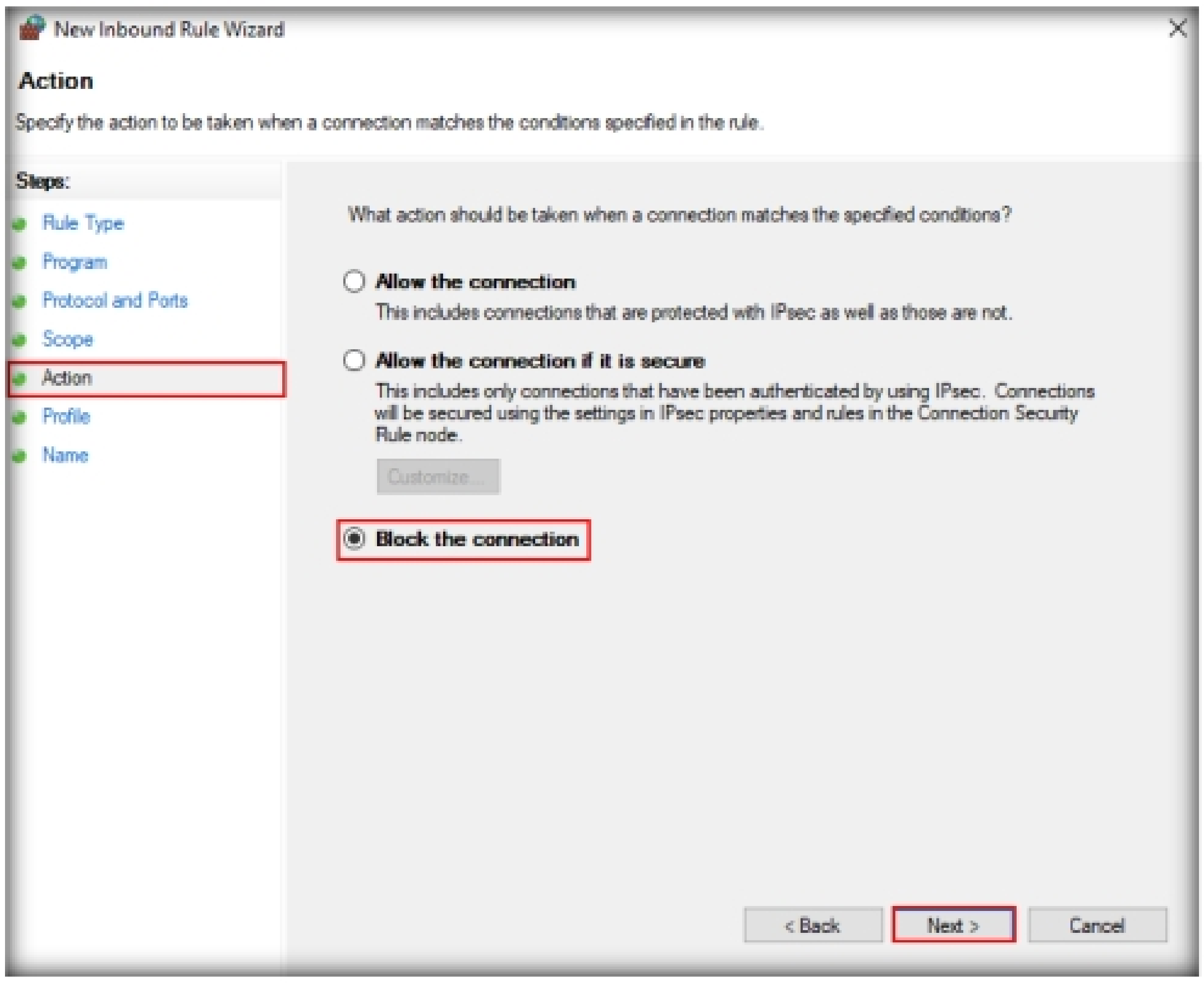
10.10.10.13

Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
Add...
Edit...
Remove
Customize...
Add...
Edit...
Remove
< Back
Next >
Cancel

Figure 2.1.9: Scope wizard

12. In the **Action** section, choose the **Block the connection** radio button and click **Next**.

13. By doing this, we are blocking all incoming traffic that comes through the **Parrot Security** virtual machine.



New Inbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

What action should be taken when a connection matches the specified conditions?

○ **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

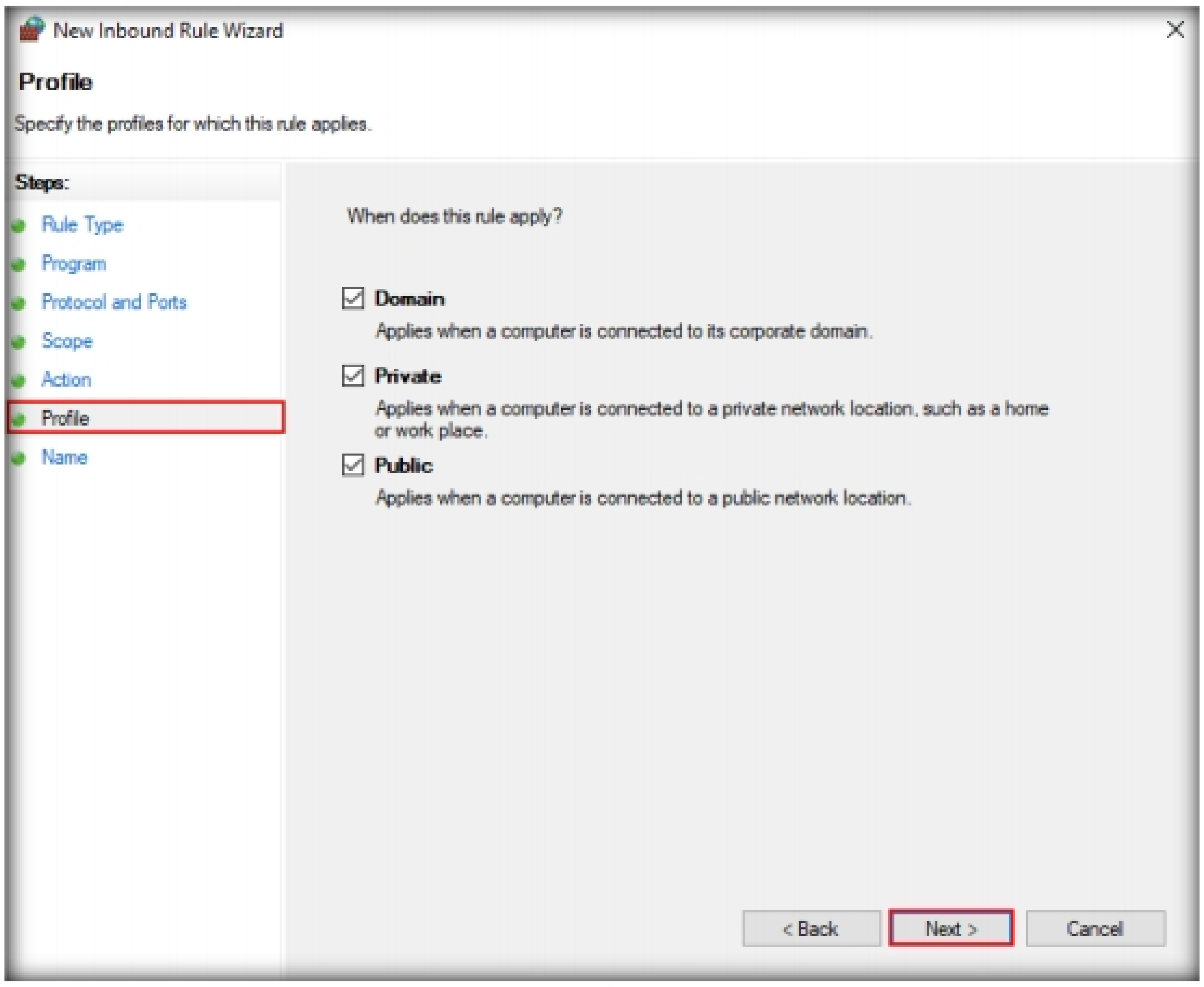
○ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

● **Block the connection**

Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
Customize...
< Back
Next >
Cancel

Figure 2.1.10: Action wizard

14. In the **Profile** section, leave the settings on default and click **Next**. By doing this, the newly created rule will apply to all profiles.



New Inbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

When does this rule apply?

☑ **Domain**
Applies when a computer is connected to its corporate domain.

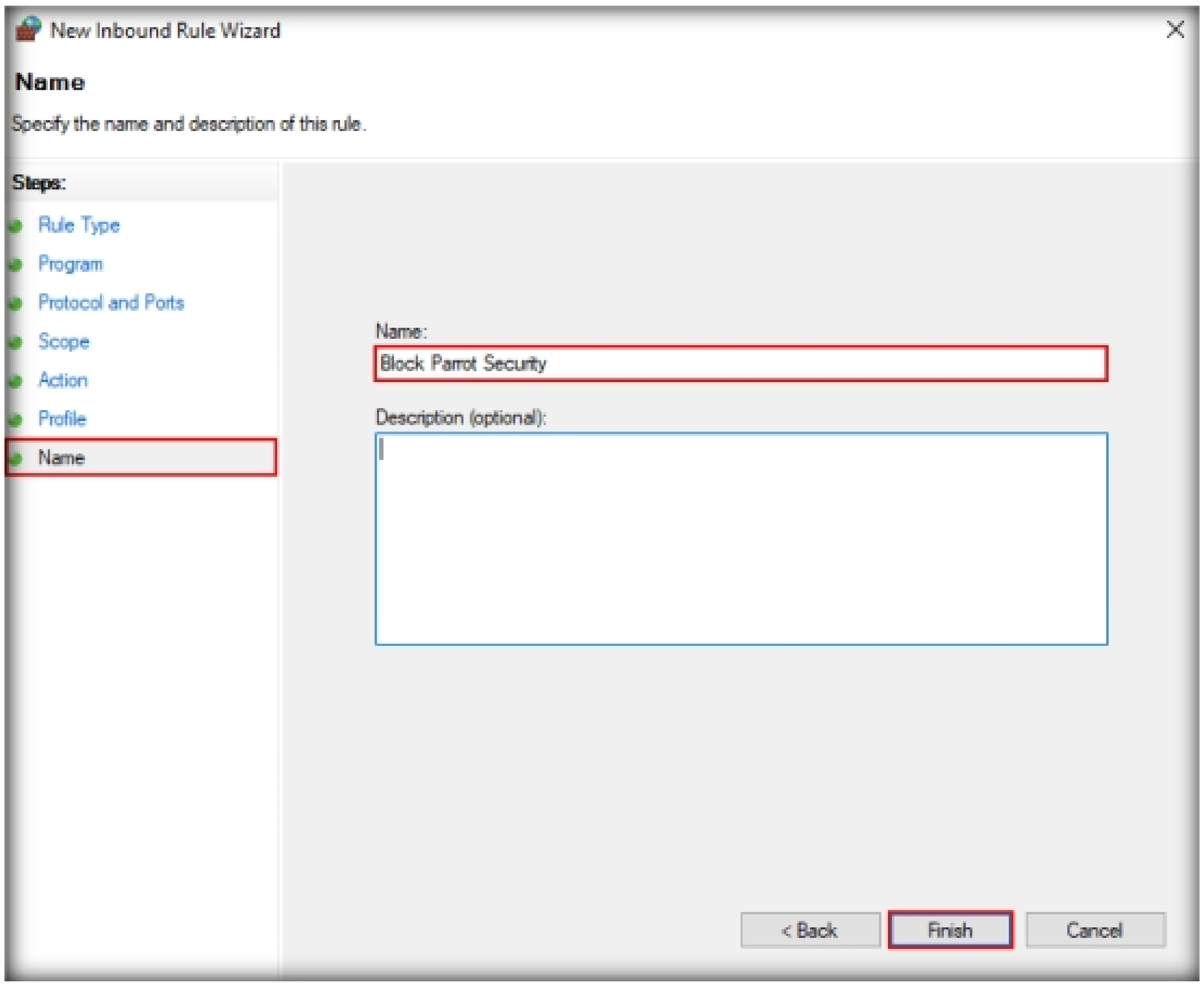
☑ **Private**
Applies when a computer is connected to a private network location, such as a home or work place.

☑ **Public**
Applies when a computer is connected to a public network location.

Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
< Back
Next >
Cancel

Figure 2.1.11: Profile wizard

15. In the **Name** section, provide any name to the rule and click **Finish**.



New Inbound Rule Wizard

Name

Specify the name and description of this rule.

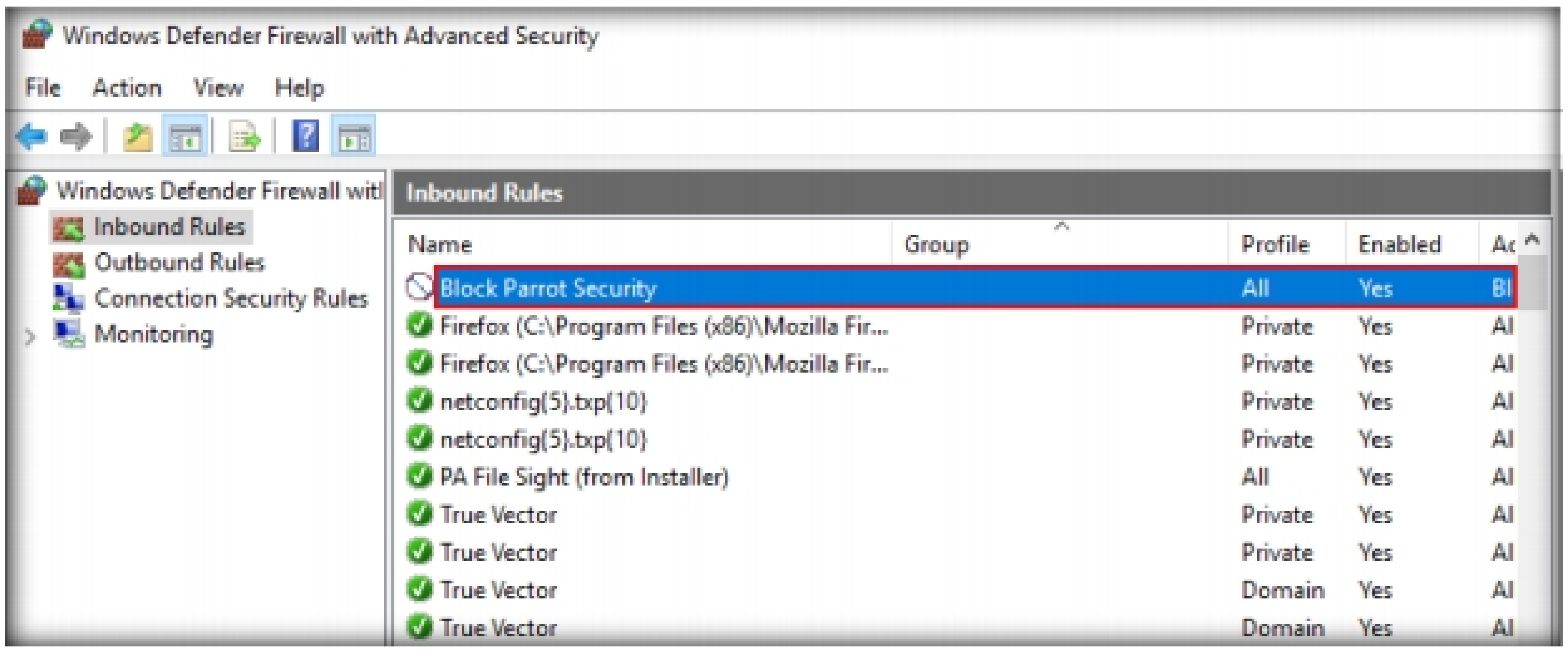
Name:
Block Parrot Security

Description (optional):

Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
< Back
Finish
Cancel

Figure 2.1.12: Name wizard

16. The newly created inbound rule has been configured to the **Windows 10** Firewall. Now, any **Incoming traffic** coming through the **Parrot Security** virtual machine will be **blocked** by the **Windows 10** Firewall.


Windows Defender Firewall with Advanced Security
File
Action
View
Help
Windows Defender Firewall witl
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules

Name	Group	Profile	Enabled	Ac
Block Parrot Security		All	Yes	Bl
Firefox (C:\Program Files (x86)\Mozilla Fir...		Private	Yes	Al
Firefox (C:\Program Files (x86)\Mozilla Fir...		Private	Yes	Al
netconfig{5}.txp{10}		Private	Yes	Al
netconfig{5}.txp{10}		Private	Yes	Al
PA File Sight (from Installer)		All	Yes	Al
True Vector		Private	Yes	Al
True Vector		Private	Yes	Al
True Vector		Domain	Yes	Al
True Vector		Domain	Yes	Al

Figure 2.1.13: New rule created

17. Close all open windows in the **Windows 10** machine and switch to the **Parrot Security** virtual machine.

18. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

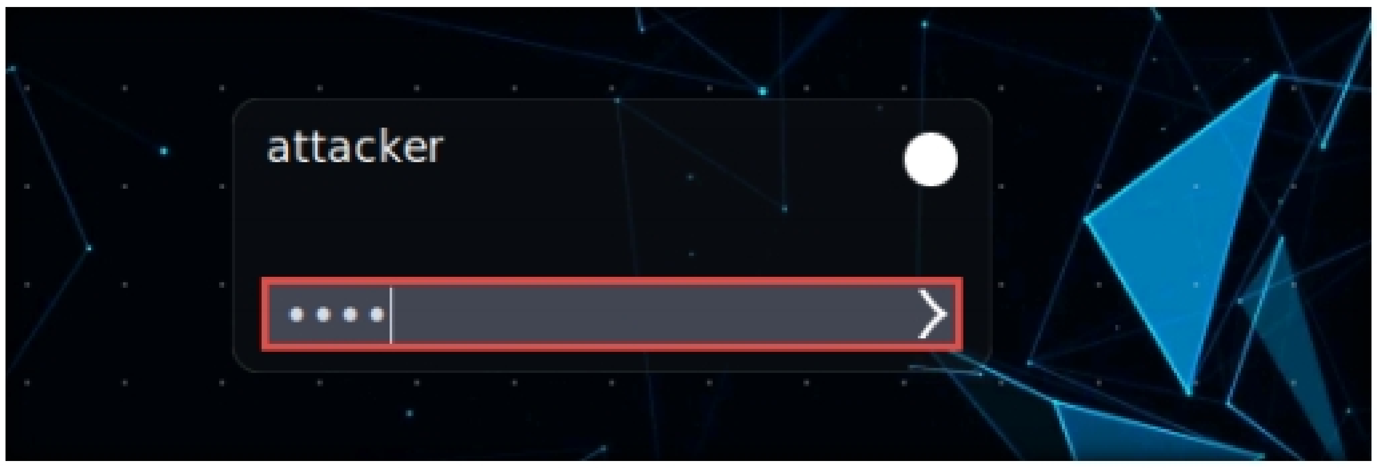


Figure 2.1.14: Parrot Security login

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window

19. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

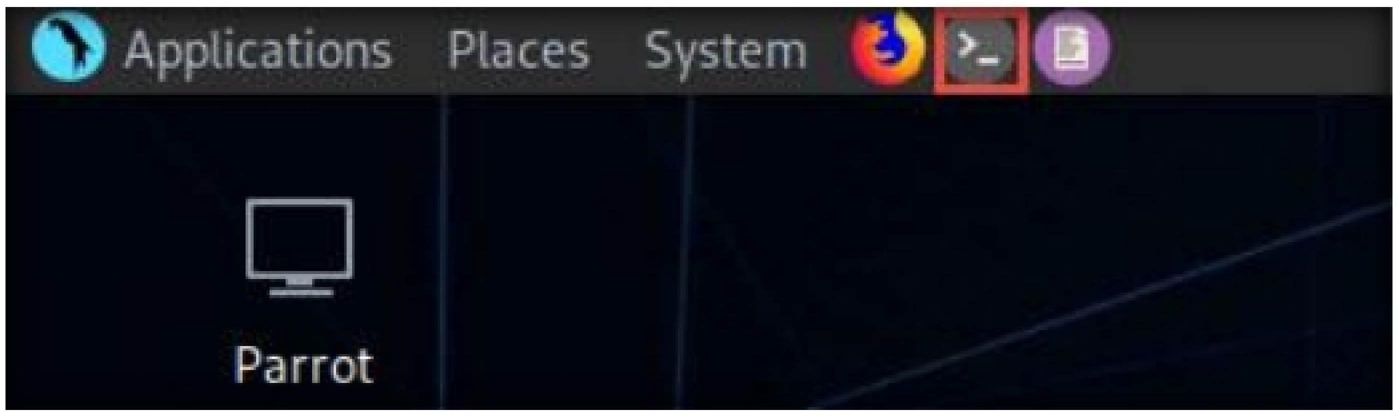

Applications
Places
System
Parrot

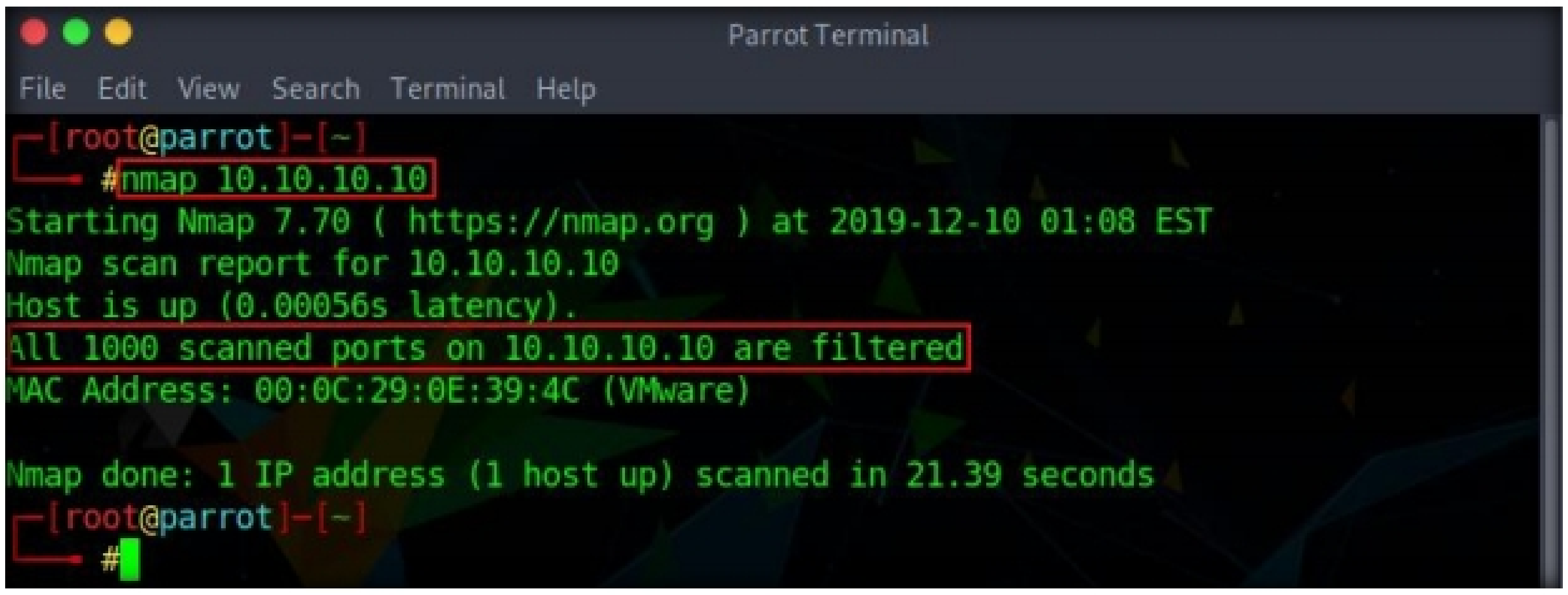
Figure 2.1.15: MATE Terminal launching

20. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
21. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

22. Now, type **cd** and press **Enter** to jump to the root directory.
23. We will now perform a basic Nmap scan on Windows 10 machine.
24. Type **nmap 10.10.10.10** and press **Enter**. As the Firewall is turned on in the **Windows 10** machine, the output of the Nmap scan shows that all the 1,000 scanned ports on **10.10.10.10** are filtered.

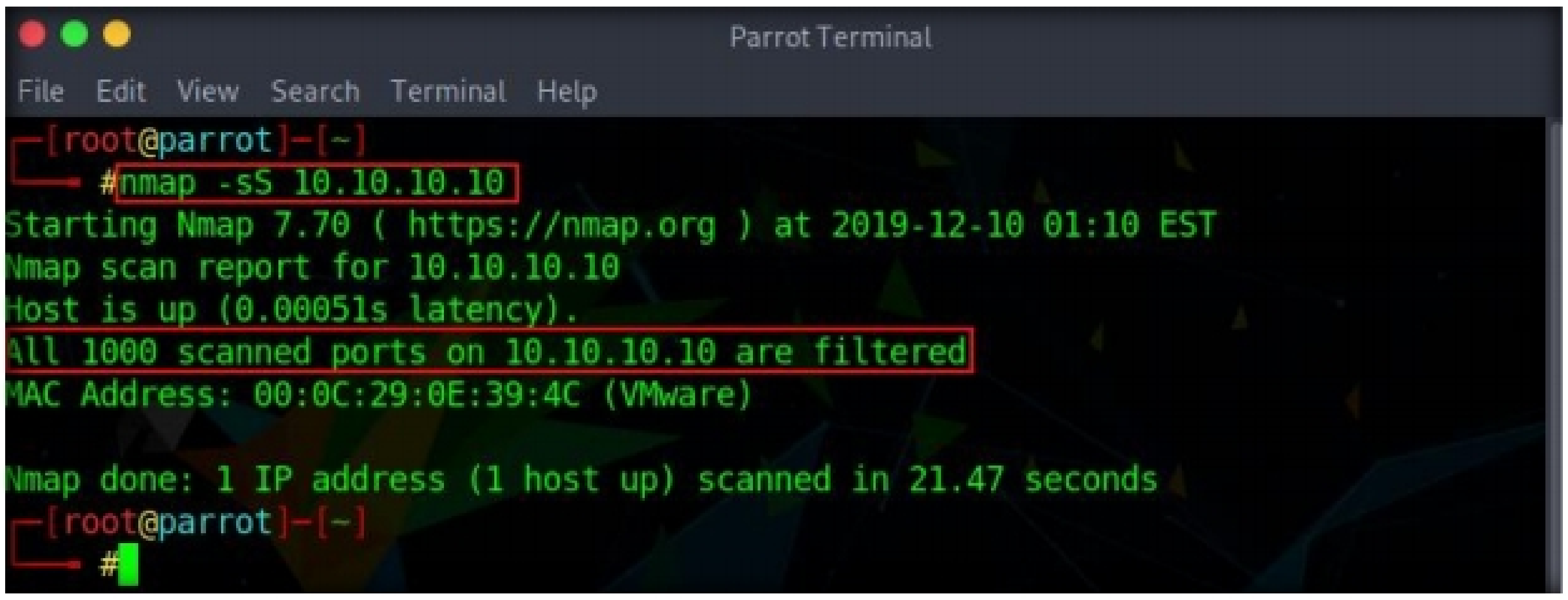
Note: The IP address of the **Windows 10** machine may differ in your lab environment.



```
┌─[root@parrot]─[~]
└──╼ #nmap 10.10.10.10
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-10 01:08 EST
Nmap scan report for 10.10.10.10
Host is up (0.00056s latency).
All 1000 scanned ports on 10.10.10.10 are filtered
MAC Address: 00:0C:29:0E:39:4C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.39 seconds
┌─[root@parrot]─[~]
└──╼ #
```

Figure 2.1.16: Nmap basic scan

25. We will now perform **TCP SYN Port Scan** on the **Windows 10** machine and observe the results.
26. Type **nmap -sS 10.10.10.10** and press **Enter**. Observe that the results are the same as when the Windows 10 Firewall is turned on.

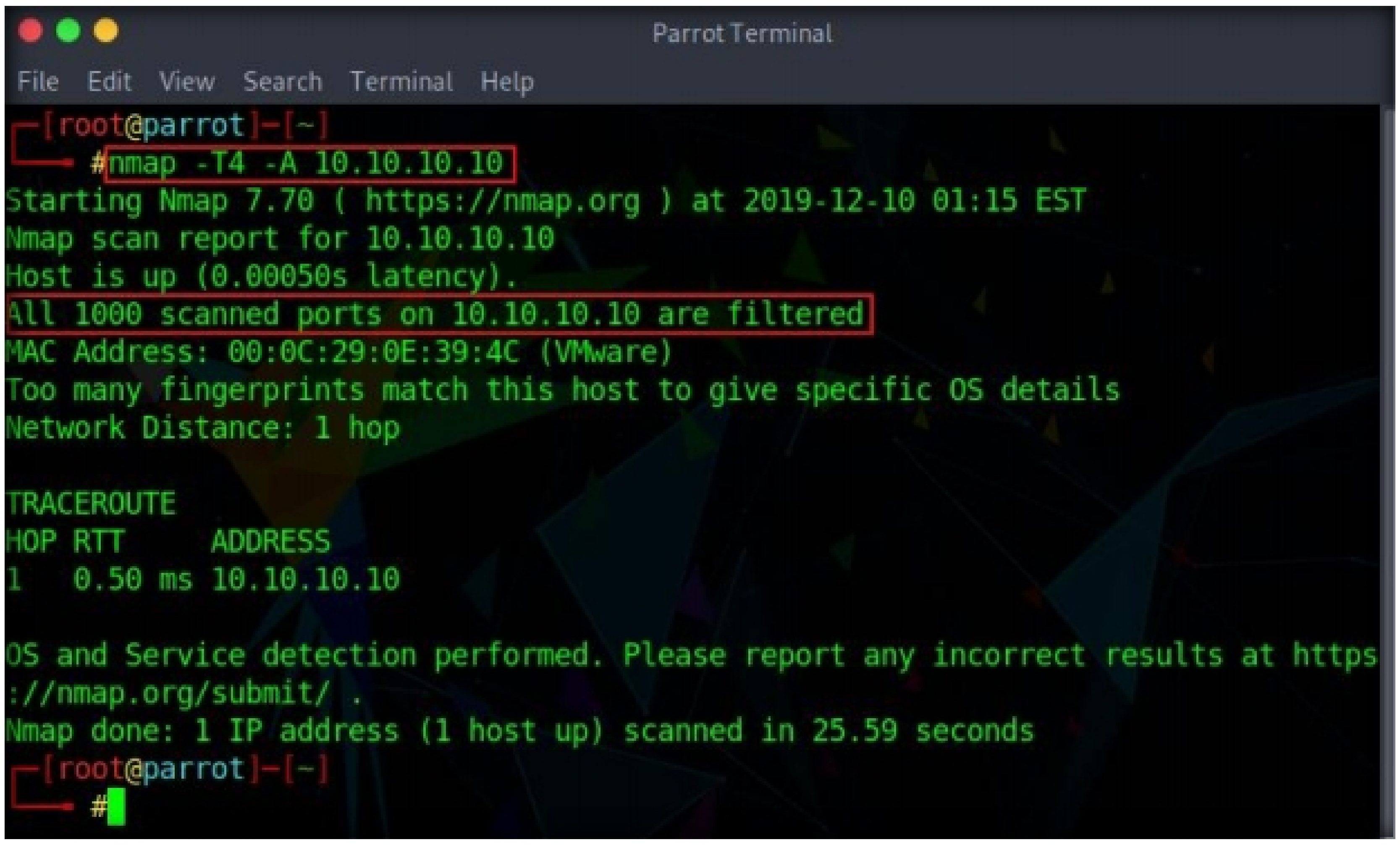


```
┌─[root@parrot]─[~]
└──╼ #nmap -sS 10.10.10.10
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-10 01:10 EST
Nmap scan report for 10.10.10.10
Host is up (0.00051s latency).
All 1000 scanned ports on 10.10.10.10 are filtered
MAC Address: 00:0C:29:0E:39:4C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.47 seconds
┌─[root@parrot]─[~]
└──╼ #
```

Figure 2.1.17: Nmap SYN scan

27. Now, perform **INTENSE Scan**. Type **nmap -T4 -A 10.10.10.10** and press **Enter**. We still receive the same result as when the Firewall is turned on.

Note: Here, **-T4** switch refers to the Aggressive (4) speeds scans and **-A** switch enables OS detection, version detection, script scanning, and traceroute.

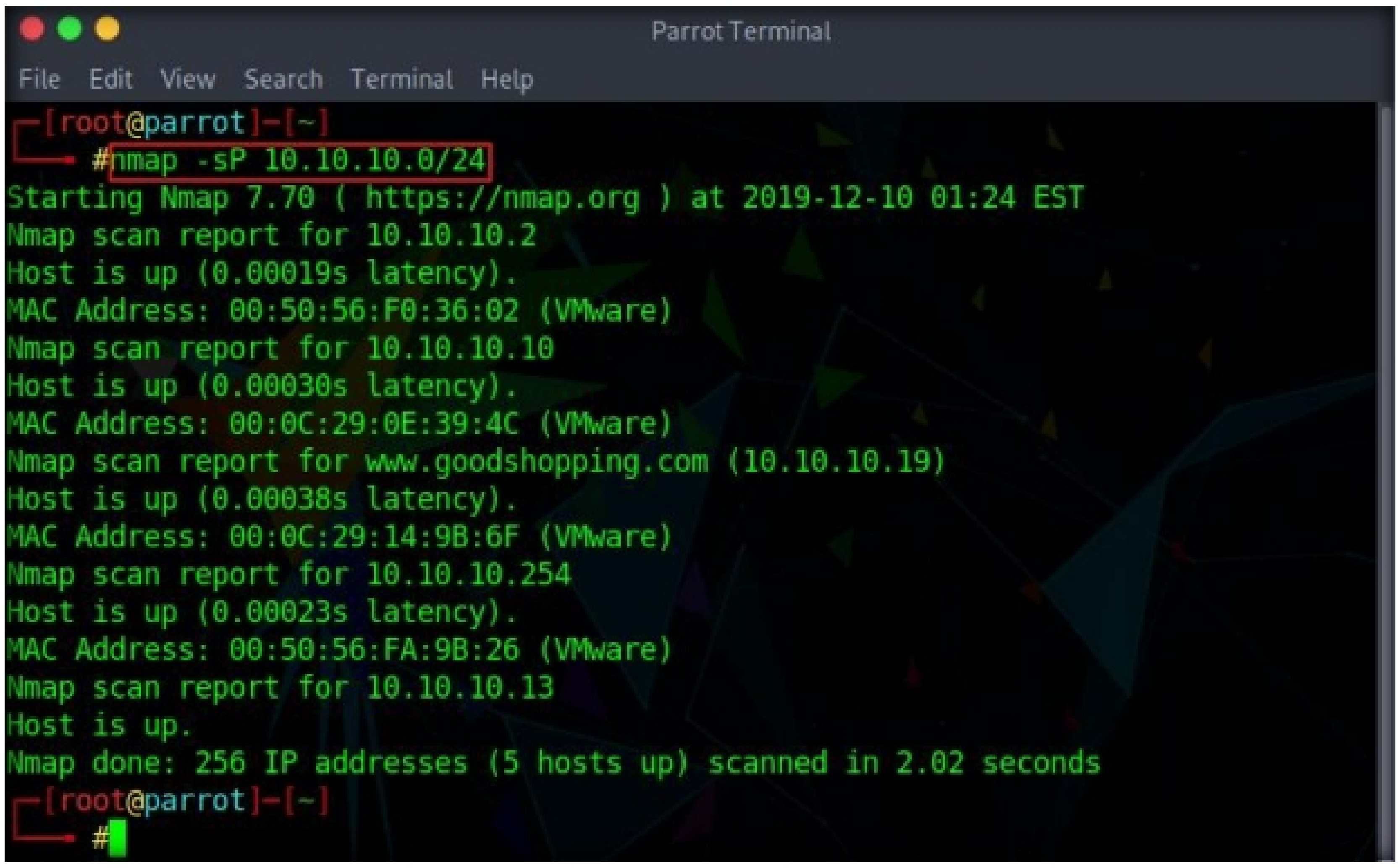


```
┌─[root@parrot]─[~]
└──╼ #nmap -T4 -A 10.10.10.10
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-10 01:15 EST
Nmap scan report for 10.10.10.10
Host is up (0.00050s latency).
All 1000 scanned ports on 10.10.10.10 are filtered
MAC Address: 00:0C:29:0E:39:4C (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.50 ms 10.10.10.10

OS and Service detection performed. Please report any incorrect results at https
://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.59 seconds
┌─[root@parrot]─[~]
└──╼ #
```

Figure 2.1.18: Nmap Intense scan

28. We will now perform a **Ping Sweep** scan on the subnet to discover the live machines in the network. Type **nmap -sP 10.10.10.0/24** and press **Enter**. In the output of the Nmap, you will be able to find the live machines on the network, as shown in the screenshot.

29. As per the scan result, you can observe that the Windows Server 2019 machine is Active (10.10.10.19).



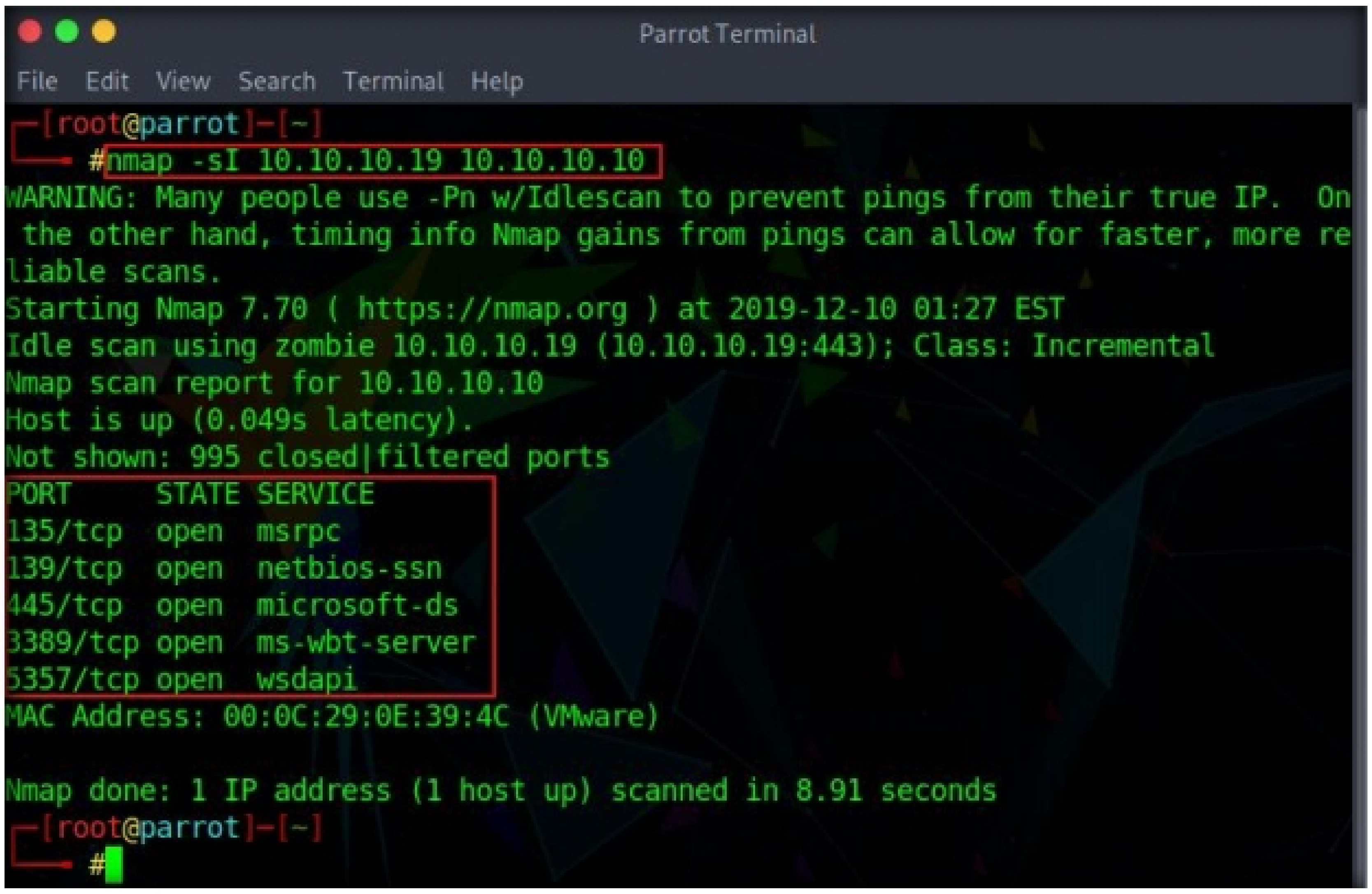
```
┌─[root@parrot]─[~]
└──╼ #nmap -sP 10.10.10.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-10 01:24 EST
Nmap scan report for 10.10.10.2
Host is up (0.00019s latency).
MAC Address: 00:50:56:F0:36:02 (VMware)
Nmap scan report for 10.10.10.10
Host is up (0.00030s latency).
MAC Address: 00:0C:29:0E:39:4C (VMware)
Nmap scan report for www.goodshopping.com (10.10.10.19)
Host is up (0.00038s latency).
MAC Address: 00:0C:29:14:9B:6F (VMware)
Nmap scan report for 10.10.10.254
Host is up (0.00023s latency).
MAC Address: 00:50:56:FA:9B:26 (VMware)
Nmap scan report for 10.10.10.13
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.02 seconds
┌─[root@parrot]─[~]
└──╼ #
```

Figure 2.1.19: Nmap Ping Sweep scan

30. Now, perform a **Zombie Scan**. Type **nmap -sI 10.10.10.19 10.10.10.10** and press **Enter**. You can see that various ports and services are open, as shown in the screenshot.

Note: The scan results may differ in your lab environment while performing this task.

Note: You can perform a Zombie scan by choosing any of the IPs that are obtained in the ping sweep scan. In this lab, we are choosing Windows Server 2019 as the Zombie.



```
┌─[root@parrot]─[~]
└──╼ #nmap -sI 10.10.10.19 10.10.10.10
WARNING: Many people use -Pn w/Idlescan to prevent pings from their true IP.  On
 the other hand, timing info Nmap gains from pings can allow for faster, more re
liable scans.
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-10 01:27 EST
Idle scan using zombie 10.10.10.19 (10.10.10.19:443); Class: Incremental
Nmap scan report for 10.10.10.10
Host is up (0.049s latency).
Not shown: 995 closed|filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
MAC Address: 00:0C:29:0E:39:4C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 8.91 seconds
┌─[root@parrot]─[~]
└──╼ #
```

Figure 2.1.20: Nmap Zombie scan

31. Delete the newly created rule in the **Windows Defender Firewall with Advanced Security** window in the **Windows 10** virtual machine.

32. **Turn off the Windows Defender Firewall** for all **Profiles** in the **Windows 10** virtual machine.

33. Close all open windows in each virtual machine.

34. Turn off the **Parrot Security** virtual machine.

TASK 2

Bypass Firewall Rules using HTTP/FTP Tunneling

Here, we will learn how networks can be scanned, and how to use HTTPort and HTTHost to bypass firewall restrictions and access files.

Note: Ensure that the **Windows Server 2019** and **Windows 10** virtual machines are running.

TASK 2.1

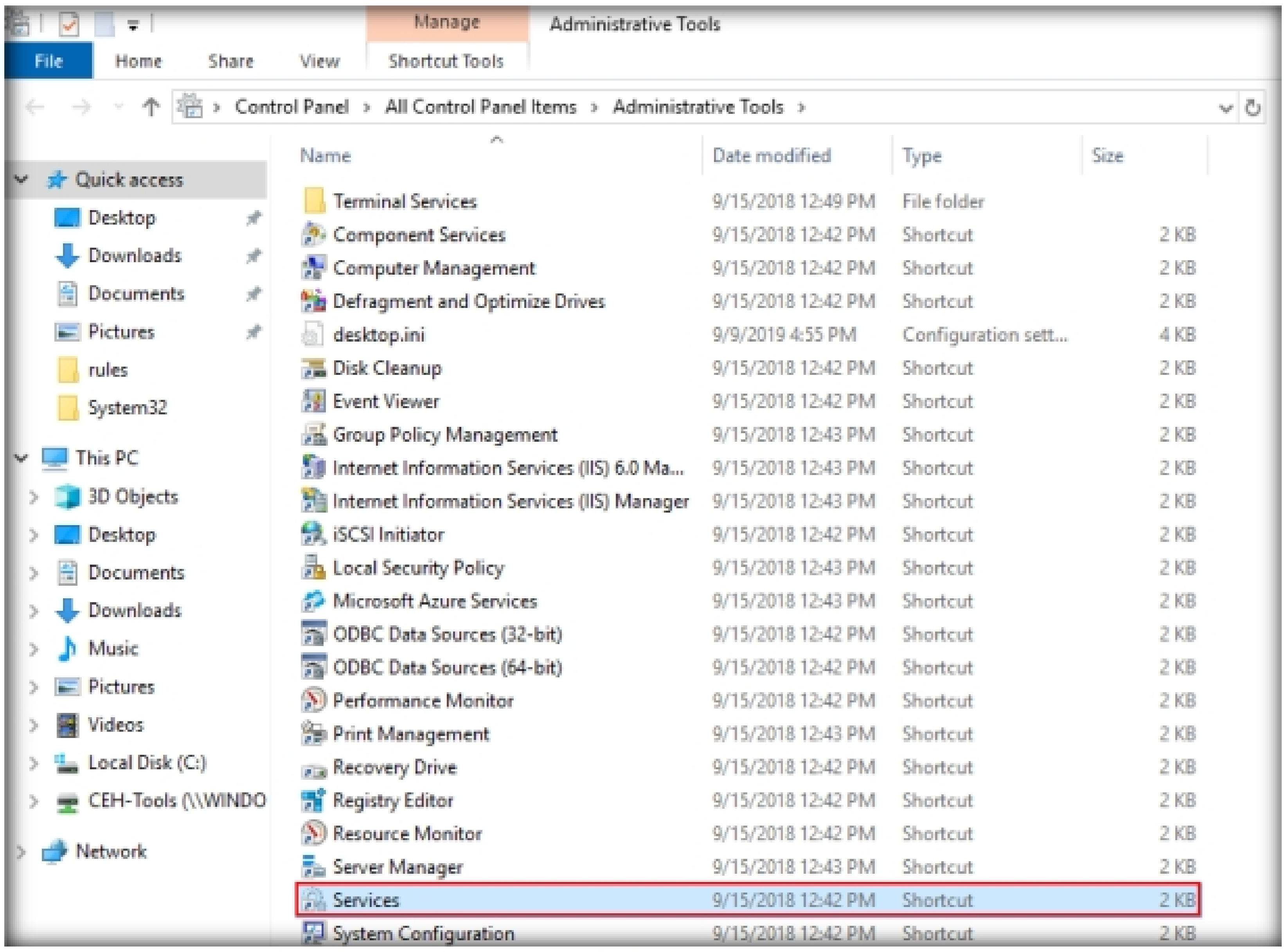
Stop World Wide Web Publishing Service

1. Turn on the **Windows Server 2016** virtual machine and log in with the credentials **Administrator** and **Pa$$w0rd**.

2. Now, you must ensure that **IIS Admin Service** and **World Wide Web Publishing services** are not running

HTTP tunneling technology allows attackers to perform various Internet tasks despite the restrictions imposed by firewalls. This method can be implemented if the target company has a public web server with port 80 used for HTTP traffic that is unfiltered by its firewall. This technology encapsulates data inside HTTP traffic (port 80). Many firewalls do not examine the payload of an HTTP packet to confirm that it is legitimate, thus it is possible to tunnel traffic via TCP port 80.

3. Click **Start** and click the **Windows Administrative Tools** app. The **Windows Administrative Tools** window appears; double-click **Services** to launch.

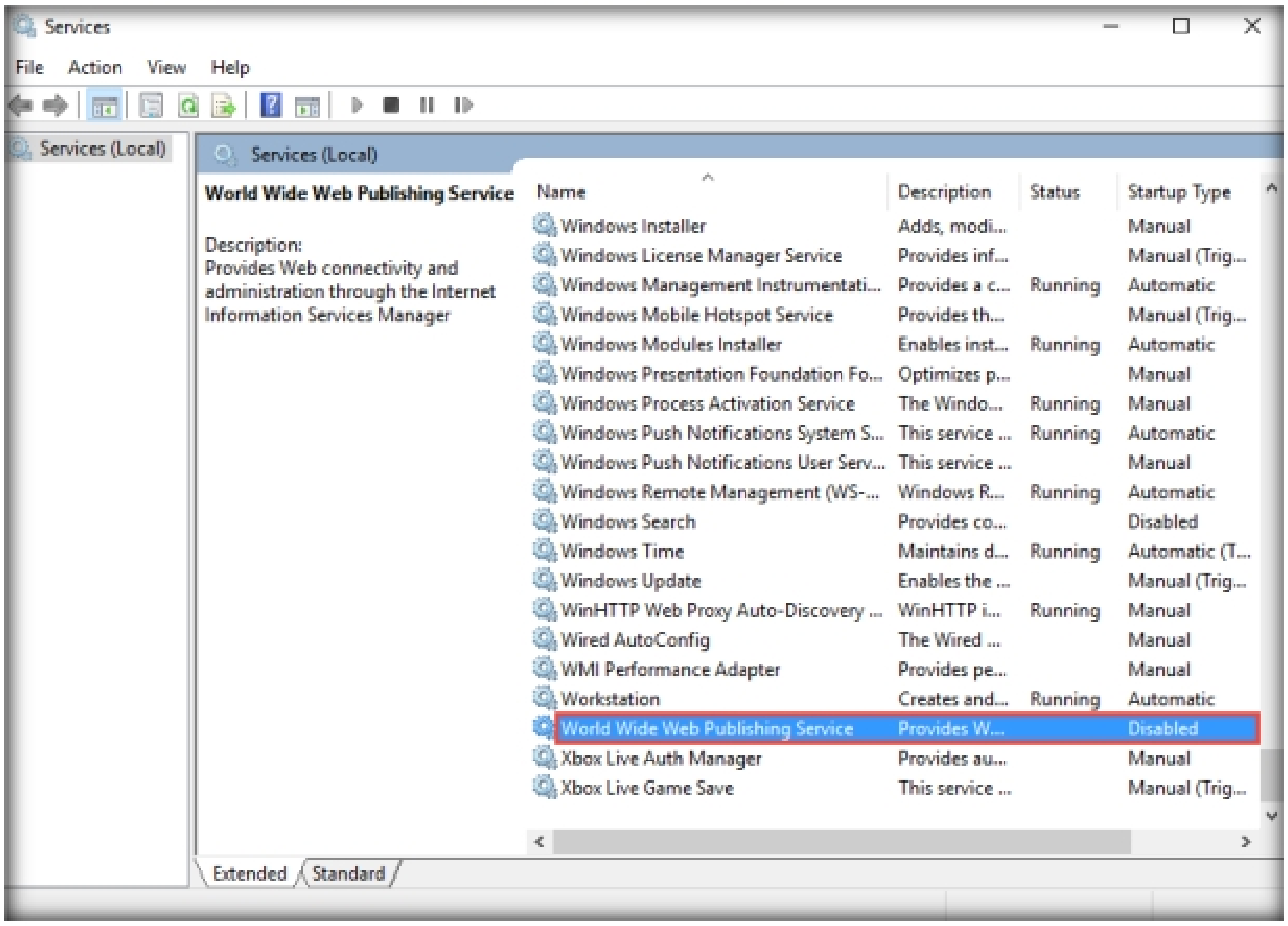


Name	Date modified	Type	Size
Terminal Services	9/15/2018 12:49 PM	File folder	
Component Services	9/15/2018 12:42 PM	Shortcut	2 KB
Computer Management	9/15/2018 12:42 PM	Shortcut	2 KB
Defragment and Optimize Drives	9/15/2018 12:42 PM	Shortcut	2 KB
desktop.ini	9/9/2019 4:55 PM	Configuration sett...	4 KB
Disk Cleanup	9/15/2018 12:42 PM	Shortcut	2 KB
Event Viewer	9/15/2018 12:42 PM	Shortcut	2 KB
Group Policy Management	9/15/2018 12:43 PM	Shortcut	2 KB
Internet Information Services (IIS) 6.0 Ma...	9/15/2018 12:43 PM	Shortcut	2 KB
Internet Information Services (IIS) Manager	9/15/2018 12:43 PM	Shortcut	2 KB
iSCSI Initiator	9/15/2018 12:42 PM	Shortcut	2 KB
Local Security Policy	9/15/2018 12:43 PM	Shortcut	2 KB
Microsoft Azure Services	9/15/2018 12:43 PM	Shortcut	2 KB
ODBC Data Sources (32-bit)	9/15/2018 12:42 PM	Shortcut	2 KB
ODBC Data Sources (64-bit)	9/15/2018 12:42 PM	Shortcut	2 KB
Performance Monitor	9/15/2018 12:42 PM	Shortcut	2 KB
Print Management	9/15/2018 12:43 PM	Shortcut	2 KB
Recovery Drive	9/15/2018 12:42 PM	Shortcut	2 KB
Registry Editor	9/15/2018 12:42 PM	Shortcut	2 KB
Resource Monitor	9/15/2018 12:42 PM	Shortcut	2 KB
Server Manager	9/15/2018 12:43 PM	Shortcut	2 KB
Services	9/15/2018 12:42 PM	Shortcut	2 KB
System Configuration	9/15/2018 12:42 PM	Shortcut	2 KB

Figure 2.2.1: Launching services

HTTPort allows users to bypass the HTTP proxy, which blocks Internet access to e-mail, instant messengers, P2P file sharing, ICQ, News, FTP, IRC, etc. Here, the Internet software is configured, so that it connects to a local PC as if it is the required remote server; HTTPort then intercepts that connection and runs it via a tunnel through the proxy.

4. In the **Services** window, scroll down to **World Wide Web Publishing Service** and you can observe that the service is **Disabled** under the **Startup Type** column, as shown in the screenshot.



World Wide Web Publishing Service

Description:
Provides Web connectivity and administration through the Internet Information Services Manager

Name	Description	Status	Startup Type
Windows Installer	Adds, modi...		Manual
Windows License Manager Service	Provides inf...		Manual (Trig...
Windows Management Instrumentati...	Provides a c...	Running	Automatic
Windows Mobile Hotspot Service	Provides th...		Manual (Trig...
Windows Modules Installer	Enables inst...	Running	Automatic
Windows Presentation Foundation Fo...	Optimizes p...		Manual
Windows Process Activation Service	The Windo...	Running	Manual
Windows Push Notifications System S...	This service ...	Running	Automatic
Windows Push Notifications User Serv...	This service ...		Manual
Windows Remote Management (WS-...	Windows R...	Running	Automatic
Windows Search	Provides co...		Disabled
Windows Time	Maintains d...	Running	Automatic (T...
Windows Update	Enables the ...		Manual (Trig...
WinHTTP Web Proxy Auto-Discovery ...	WinHTTP i...	Running	Manual
Wired AutoConfig	The Wired ...		Manual
WMI Performance Adapter	Provides pe...		Manual
Workstation	Creates and...	Running	Automatic
World Wide Web Publishing Service	Provides W...		Disabled
Xbox Live Auth Manager	Provides au...		Manual
Xbox Live Game Save	This service ...		Manual (Trig...

Figure 2.2.2: Stopping World Wide Web Publishing Service in Windows Server 2016

TASK 2.2

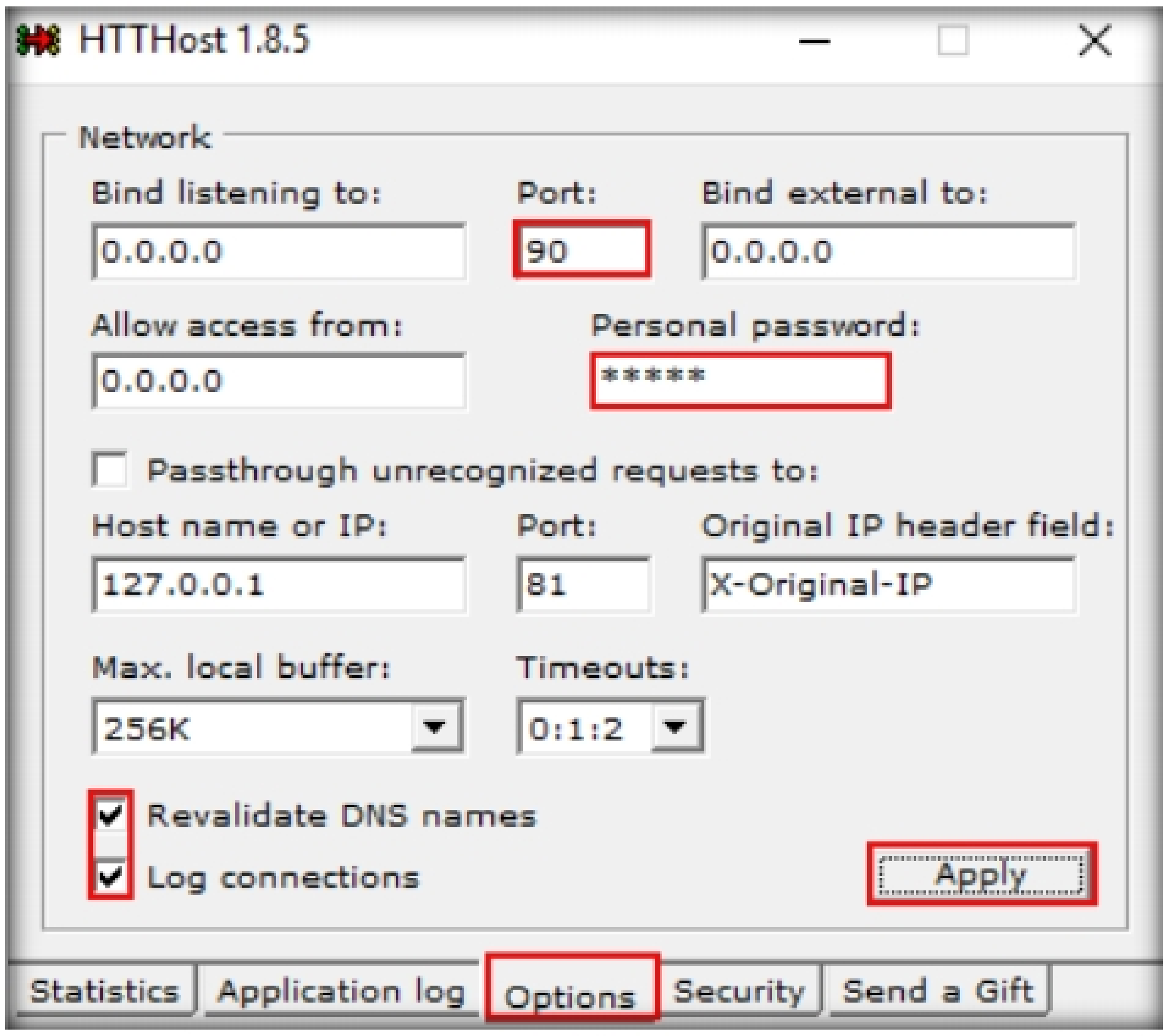
Launch and Configure HTTHost

HTTPort can work on devices such as proxies or firewalls that allow HTTP traffic. Thus, HTTPort provides access to websites and Internet apps. HTTPort performs tunneling using one of two modes: SSL/CONNECT mode and a remote host.

5. Similarly, check **IIS Admin Service**; stop the program if it is running.
6. Navigate to **Z:\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots\HTTP Tunneling Tools\HTTHost** and double-click **htthost.exe**.
7. If the **Open File - Security Warning** pop-up appears, click **Run**.
8. A **HTTHost** wizard appears; click the **Options** tab.
9. On the **Options** tab, leave **90** as the port number in the **Port** field under the **Network** section. Keep the other settings on default, except for **Personal password**, which should contain any other password. In this task, the **Personal password** is "**magic**."

Note: Typically, HTTP tunneling should be performed using port 80. Port 80 is being used to host the local websites, therefore we have used port 90 for this lab.

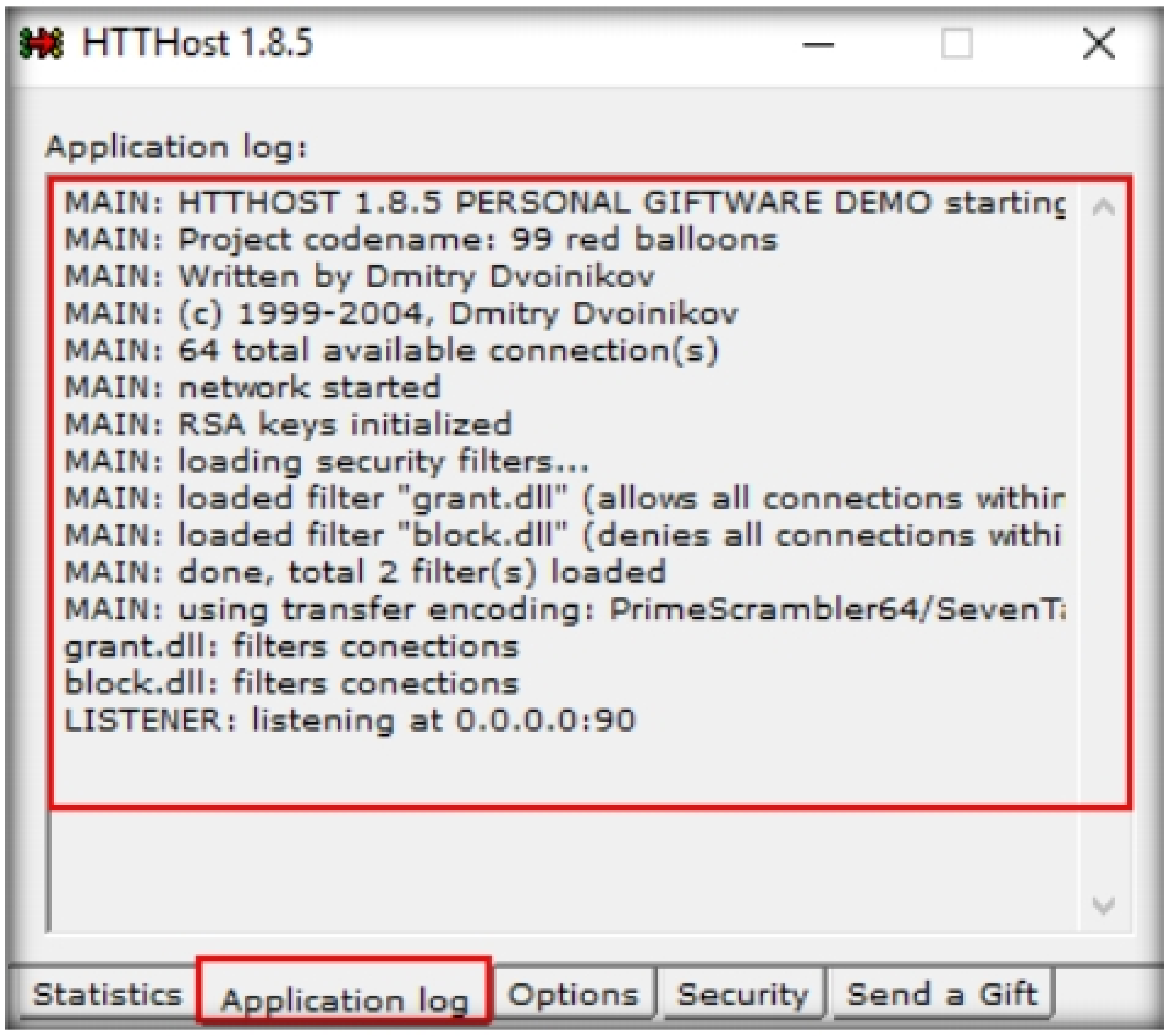
10. Ensure that **Revalidate DNS names** and **Log connections** are checked and click **Apply**.



Bind listening to: 0.0.0.0
Port: 90
Bind external to: 0.0.0.0
Allow access from: 0.0.0.0
Personal password: *****
☐ Passthrough unrecognized requests to:
Host name or IP: 127.0.0.1
Port: 81
Original IP header field: X-Original-IP
Max. local buffer: 256K
Timeouts: 0:1:2
☑ Revalidate DNS names
☑ Log connections

Figure 2.2.3: HTTHost Options tab

11. Navigate to the **Application log** tab and check if the last line is **Listener: listening at 0.0.0.0:90**, which ensures that HTTHost is running properly and has begun to listen on **port 90**.


HTTHost 1.8.5
Application log:
Statistics
Application log
Options
Security
Send a Gift

```
MAIN: HTTHOST 1.8.5 PERSONAL GIFTWARE DEMO startinc
MAIN: Project codename: 99 red balloons
MAIN: Written by Dmitry Dvoinikov
MAIN: (c) 1999-2004, Dmitry Dvoinikov
MAIN: 64 total available connection(s)
MAIN: network started
MAIN: RSA keys initialized
MAIN: loading security filters...
MAIN: loaded filter "grant.dll" (allows all connections withir
MAIN: loaded filter "block.dll" (denies all connections withi
MAIN: done, total 2 filter(s) loaded
MAIN: using transfer encoding: PrimeScrambler64/SevenT:
grant.dll: filters conections
block.dll: filters conections
LISTENER: listening at 0.0.0.0:90
```

Figure 2.2.4: HTTHost Application log section

The remote host method is capable of tunneling through any proxy. HTTPort uses a special server software called HTTHost, which is installed outside the proxy-blocked network. It is a web server, and thus when HTTPort is tunneling, it sends a series of HTTP requests to the HTTHost.

12. Now, leave **HTTHost** running, and do not turn off the **Windows Server 2016** virtual machine.

TASK 2.3

Enable Firewall and Add an Outbound Rule

13. Now, switch to the **Windows Server 2019** virtual machine and launch **Control Panel**, as shown in the screenshot.

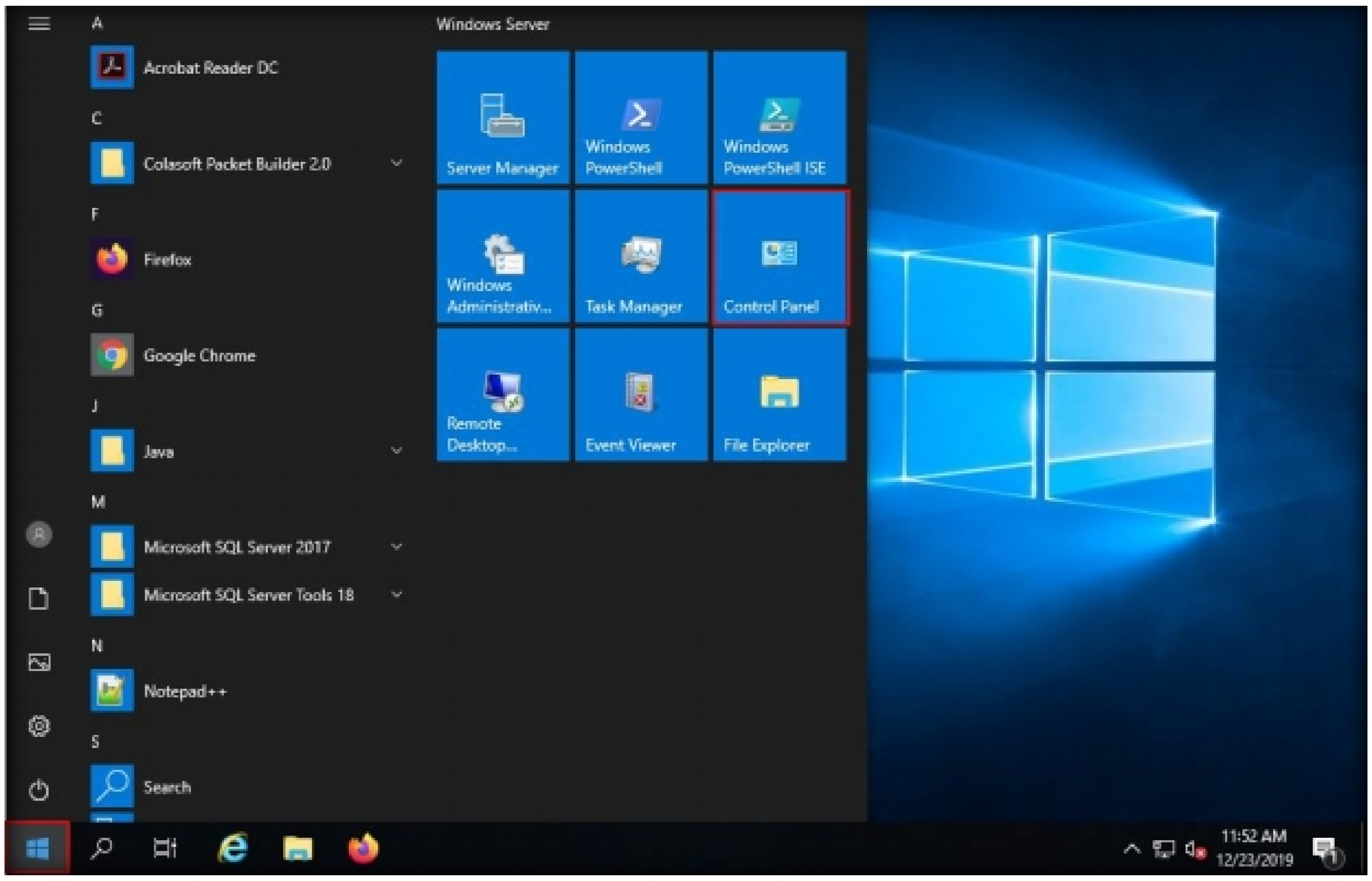

A
Acrobat Reader DC
C
Colasoft Packet Builder 2.0
F
Firefox
G
Google Chrome
J
Java
M
Microsoft SQL Server 2017
Microsoft SQL Server Tools 18
N
Notepad++
S
Search
Windows Server
Server Manager
Windows PowerShell
Windows PowerShell ISE
Windows Administrativ...
Task Manager
Control Panel
Remote Desktop...
Event Viewer
File Explorer
11:52 AM
12/23/2019

Figure 2.2.5: Launching Control Panel

🗁 The proxy responds as if the user is surfing a website and thus allows the user to do so. HTTHost, in turn, performs its half of the tunneling and communicates with the target servers. This mode is much slower, but works in the majority of cases and features strong data encryption that makes proxy logging useless.

14. The **Control Panel** window appears with all control panel items displayed. Select **Windows Defender Firewall**.

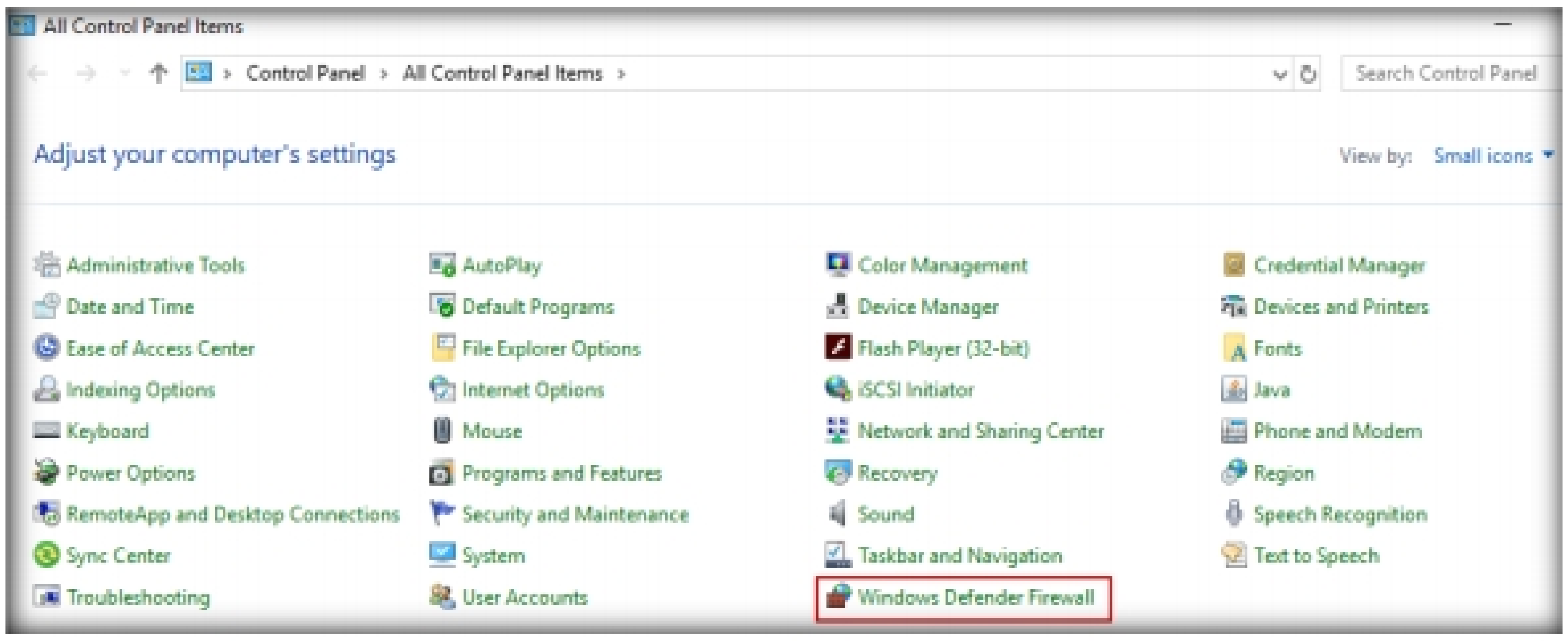
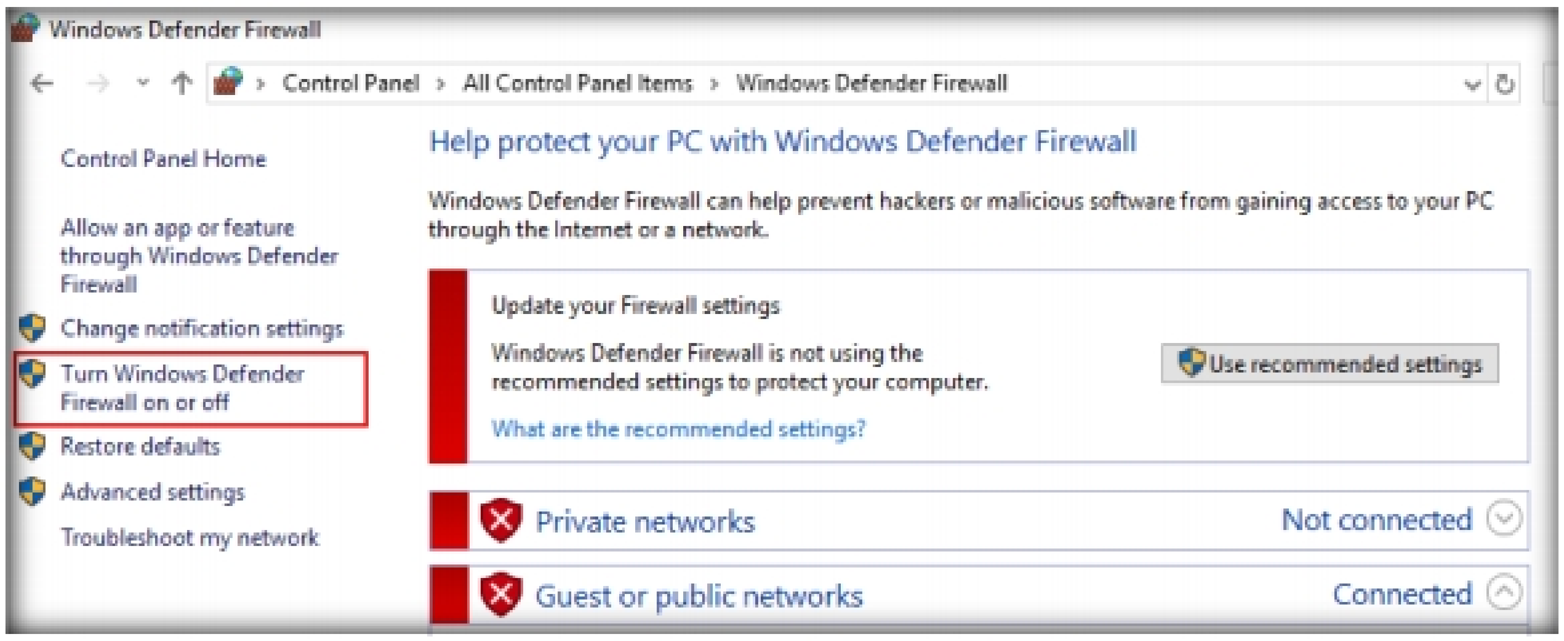

All Control Panel Items
Control Panel > All Control Panel Items >
Search Control Panel
Adjust your computer's settings
View by: Small icons
Administrative Tools
Date and Time
Ease of Access Center
Indexing Options
Keyboard
Power Options
RemoteApp and Desktop Connections
Sync Center
Troubleshooting
AutoPlay
Default Programs
File Explorer Options
Internet Options
Mouse
Programs and Features
Security and Maintenance
System
User Accounts
Color Management
Device Manager
Flash Player (32-bit)
iSCSI Initiator
Network and Sharing Center
Recovery
Sound
Taskbar and Navigation
Windows Defender Firewall
Credential Manager
Devices and Printers
Fonts
Java
Phone and Modem
Region
Speech Recognition
Text to Speech

Figure 2.2.6: Opening Windows Firewall

15. The **Windows Defender Firewall** control panel appears; click the **Turn Windows Defender Firewall on or off** link in the left pane.


Windows Defender Firewall
Control Panel > All Control Panel Items > Windows Defender Firewall
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
Help protect your PC with Windows Defender Firewall
Use recommended settings
What are the recommended settings?

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Update your Firewall settings

Windows Defender Firewall is not using the recommended settings to protect your computer.

Private networks: Not connected

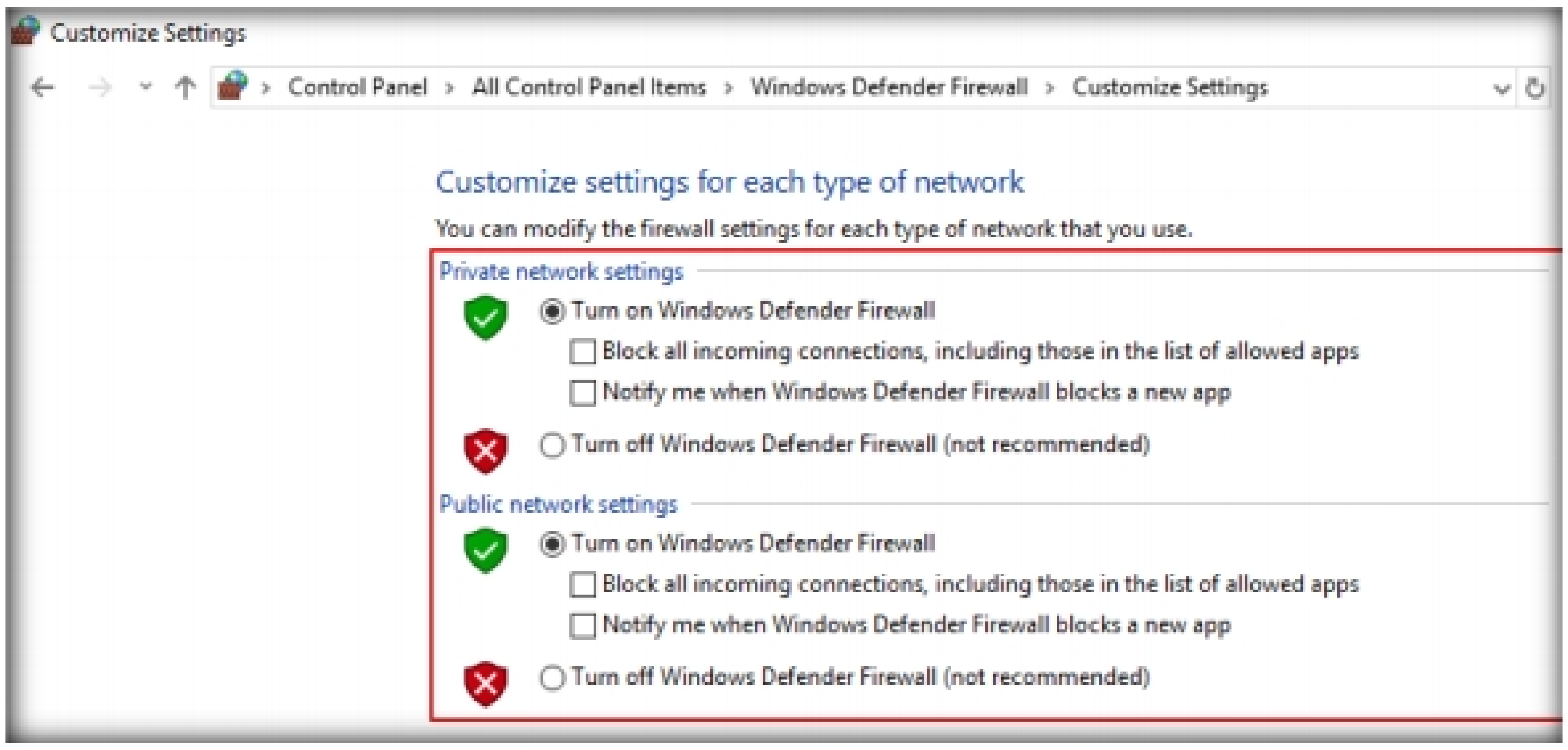
Guest or public networks: Connected

Figure 2.2.7: Configuring Windows Firewall

16. The **Customize Settings** window appears.

17. Select **Turn on Windows Defender Firewall** under **Private network settings** and **Public network settings**.

18. Click **OK**.


Customize Settings
Control Panel > All Control Panel Items > Windows Defender Firewall > Customize Settings
Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

● Turn on Windows Defender Firewall

☐ Block all incoming connections, including those in the list of allowed apps

☐ Notify me when Windows Defender Firewall blocks a new app

○ Turn off Windows Defender Firewall (not recommended)

Public network settings

● Turn on Windows Defender Firewall

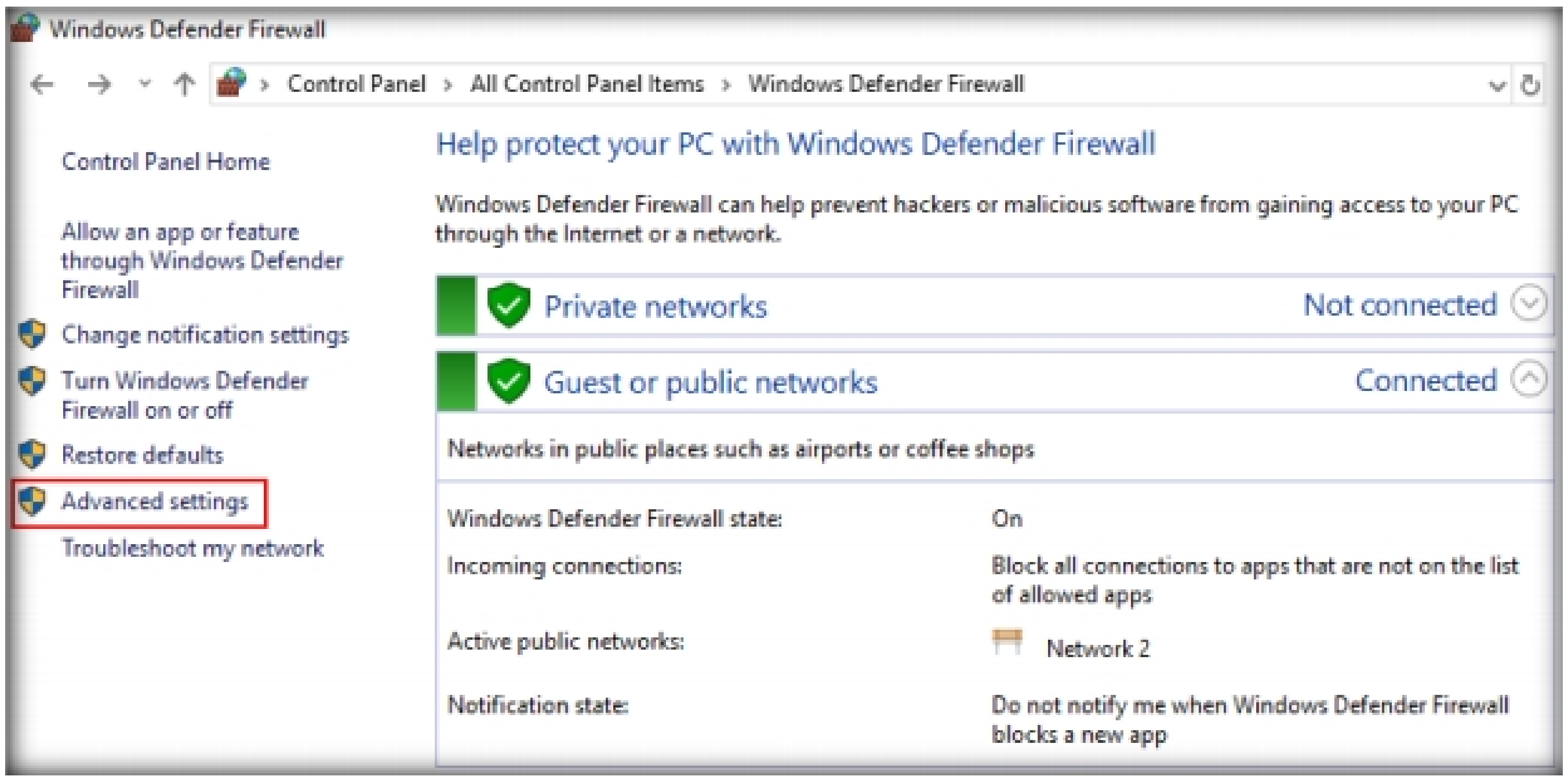
☐ Block all incoming connections, including those in the list of allowed apps

☐ Notify me when Windows Defender Firewall blocks a new app

○ Turn off Windows Defender Firewall (not recommended)

Figure 2.2.8: Configuring Windows Firewall

19. The firewall is successfully turned on. Now, click **Advanced settings** in the left pane.


Windows Defender Firewall
Control Panel > All Control Panel Items > Windows Defender Firewall
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
Private networks
Not connected
Guest or public networks
Connected

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Networks in public places such as airports or coffee shops

Windows Defender Firewall state: On

Incoming connections: Block all connections to apps that are not on the list of allowed apps

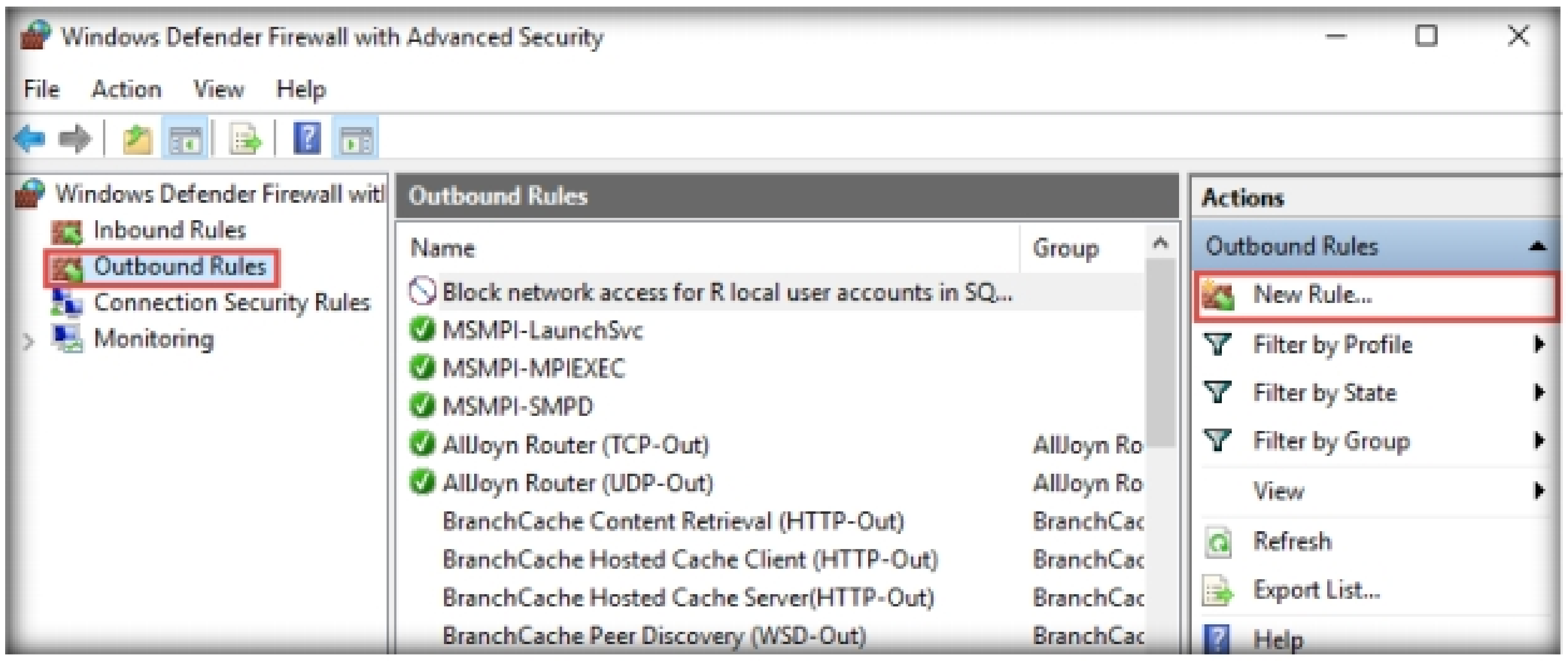
Active public networks: Network 2

Notification state: Do not notify me when Windows Defender Firewall blocks a new app

Figure 2.2.9: Configuring Advanced Windows Firewall

20. The **Windows Firewall with Advanced Security** window appears.

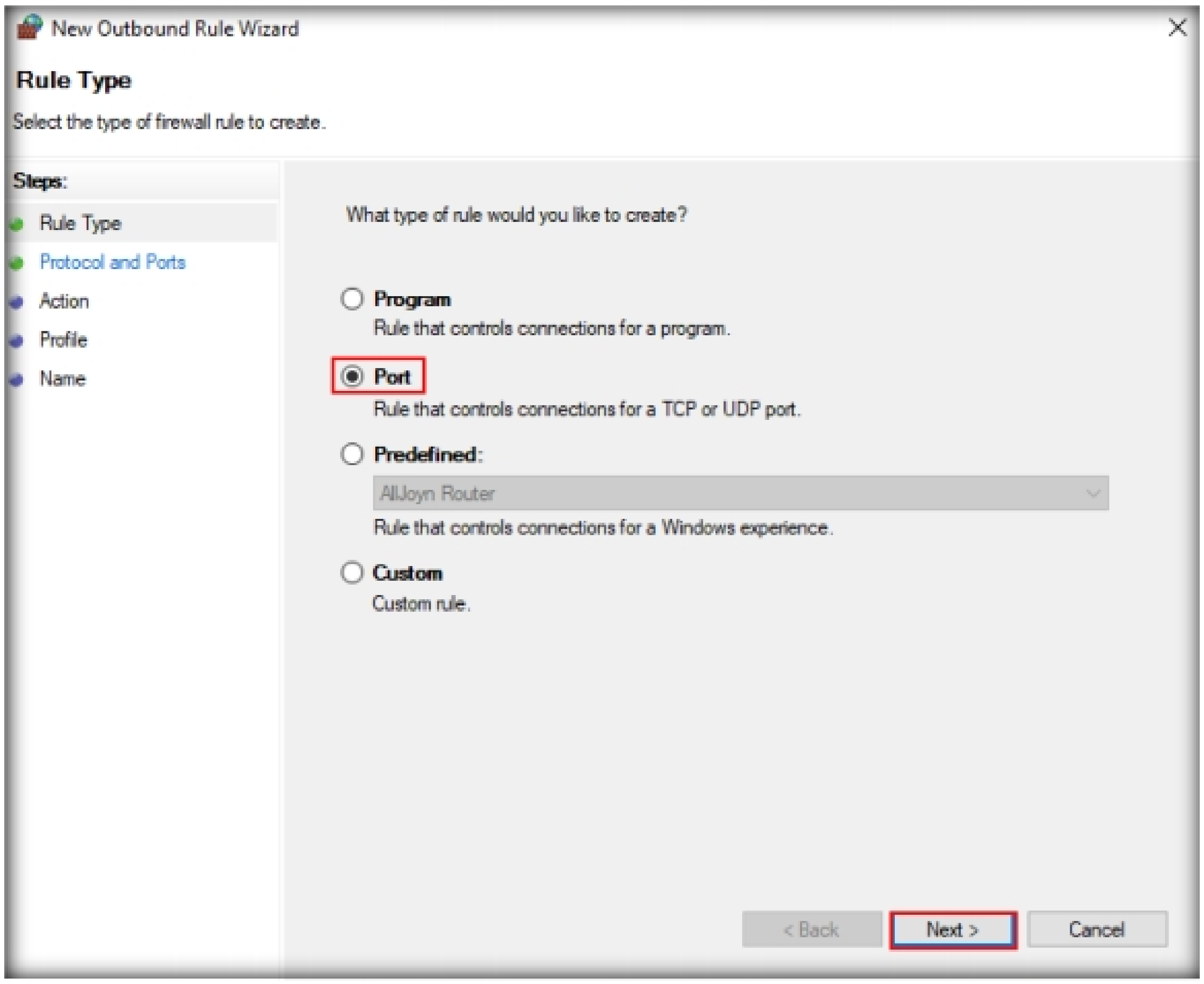
21. Select **Outbound Rules** in the left pane. A list of outbound rules is displayed. Click **New Rule...** in the right pane under **Outbound Rules**.


Windows Defender Firewall with Advanced Security
File
Action
View
Help
Windows Defender Firewall witl
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Outbound Rules
Actions
Outbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help

Name	Group
Block network access for R local user accounts in SQ...	
MSMPI-LaunchSvc	
MSMPI-MPIEXEC	
MSMPI-SMPD	
AllJoyn Router (TCP-Out)	AllJoyn Ro
AllJoyn Router (UDP-Out)	AllJoyn Ro
BranchCache Content Retrieval (HTTP-Out)	BranchCac
BranchCache Hosted Cache Client (HTTP-Out)	BranchCac
BranchCache Hosted Cache Server(HTTP-Out)	BranchCac
BranchCache Peer Discovery (WSD-Out)	BranchCac

Figure 2.2.10: Adding a new outbound rule

22. In **New Outbound Rule Wizard**, select **Port** as **Rule Type** and click **Next**.



New Outbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What type of rule would you like to create?

○ **Program**
Rule that controls connections for a program.

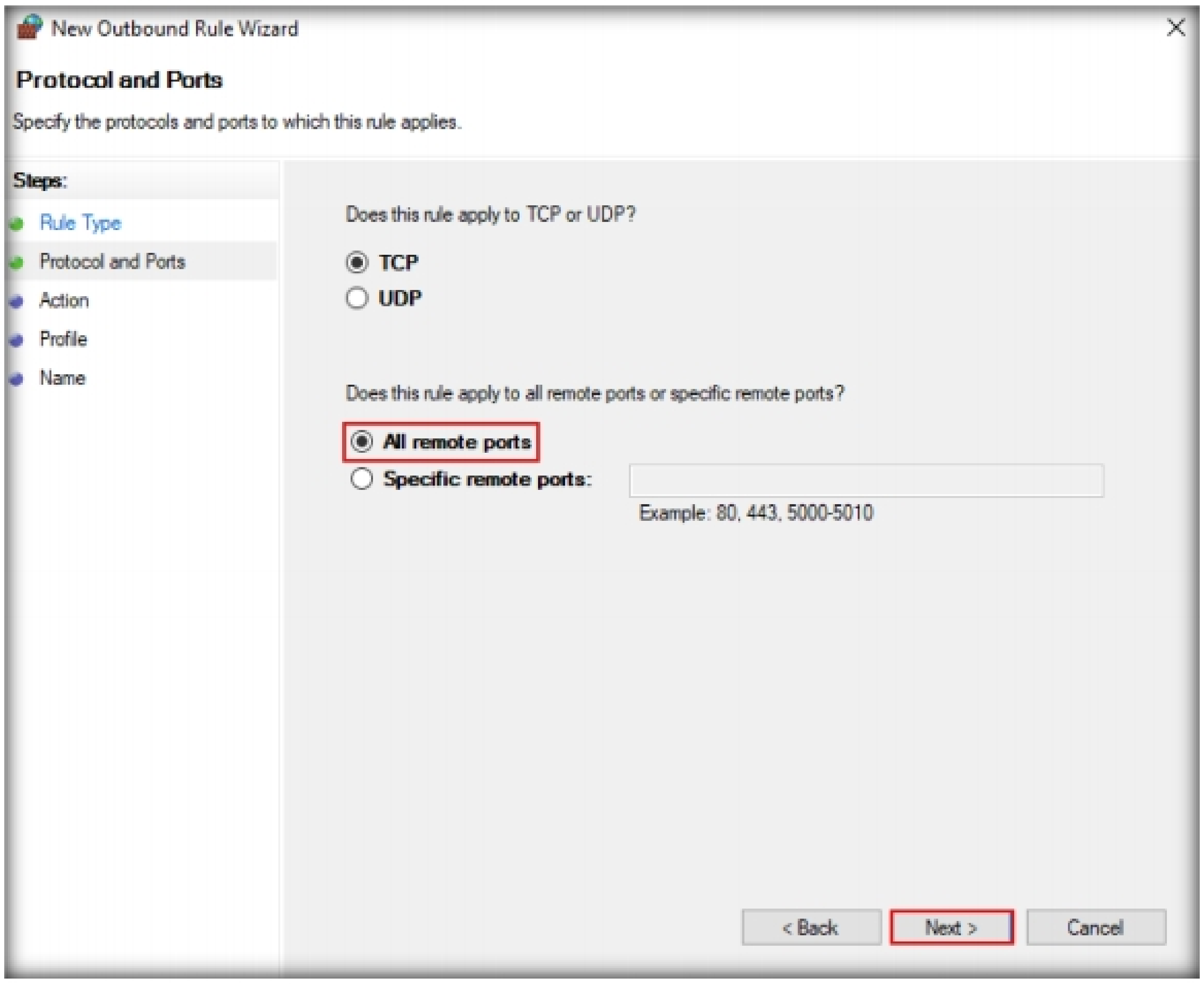
● **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
AllJoyn Router
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

Figure 2.2.11: Windows Firewall Selecting a Rule Type

23. Select **All remote ports** in **Protocol and Ports** and click **Next**.



New Outbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

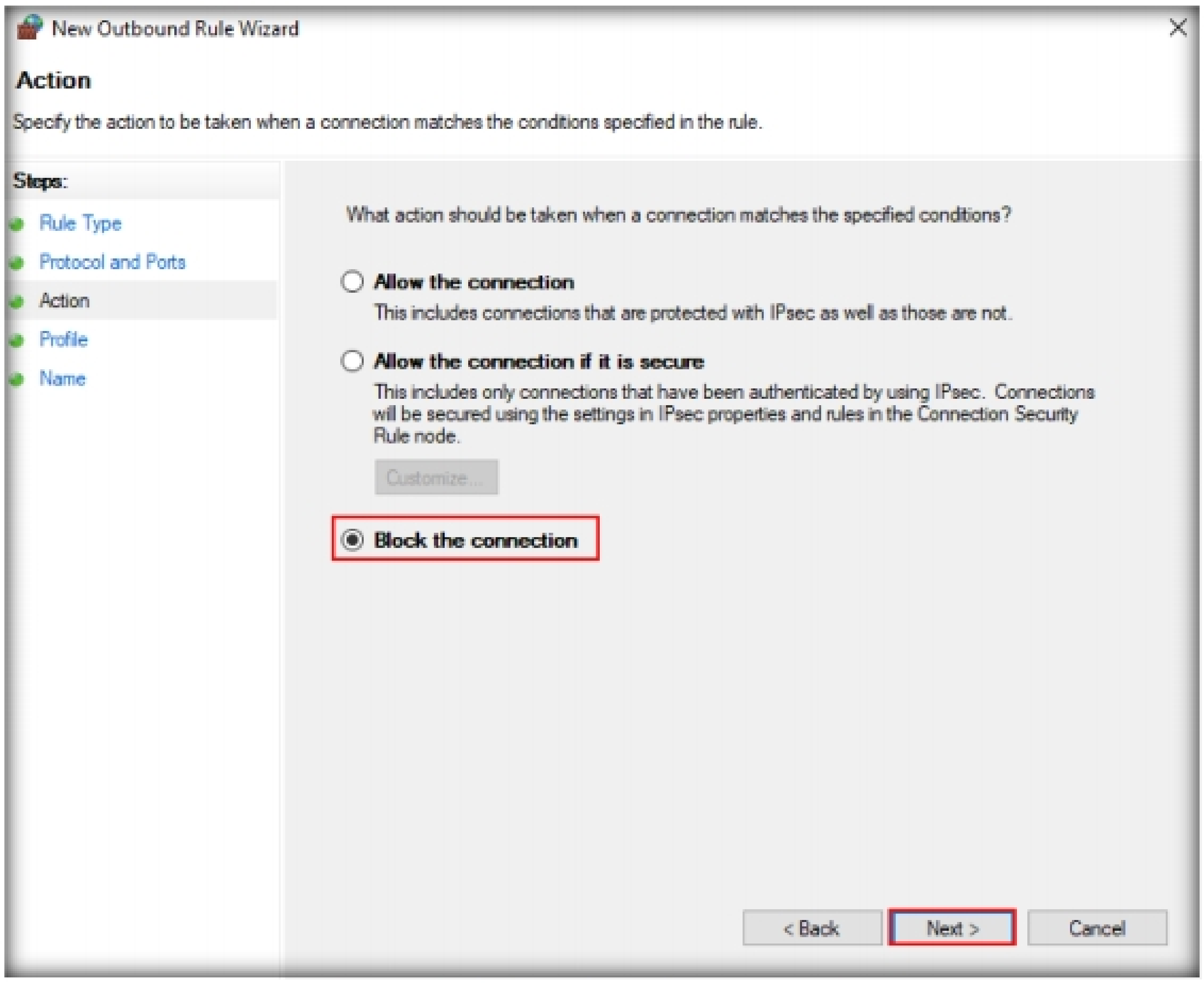
● **TCP**
○ **UDP**

Does this rule apply to all remote ports or specific remote ports?

● **All remote ports**
○ **Specific remote ports:**
Example: 80, 443, 5000-5010

Figure 2.2.12: Windows Firewall assigning Protocols and Ports

24. In **Action**, **Block the connection** is selected by default and click **Next**.


New Outbound Rule Wizard
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
Customize...
< Back
Next >
Cancel

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

What action should be taken when a connection matches the specified conditions?

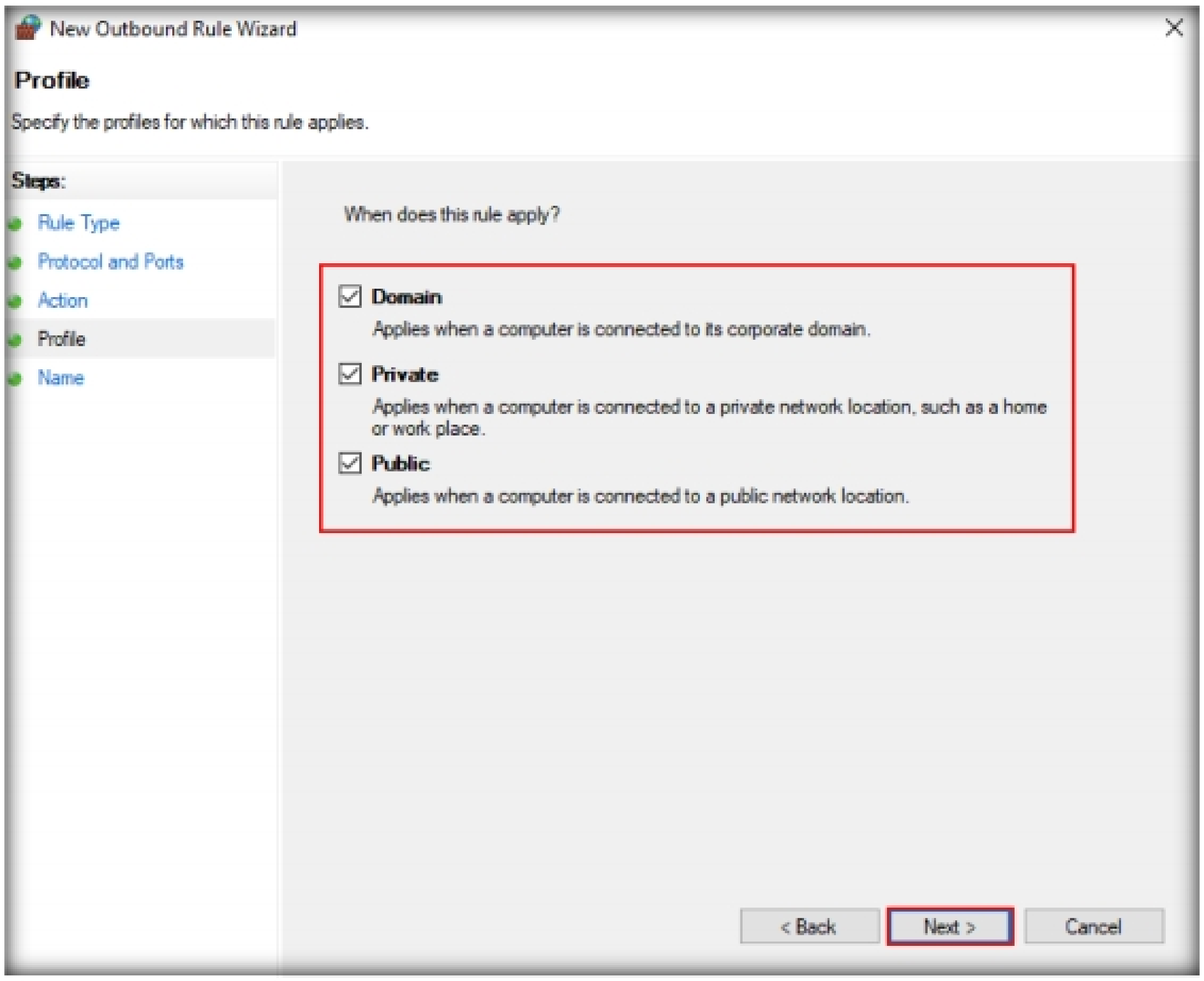
○ **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

○ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

● **Block the connection**

Figure 2.2.13: Windows Firewall setting an Action

25. In the **Profile** section, ensure that all options (**Domain**, **Private**, and **Public**) are checked and click **Next**.


New Outbound Rule Wizard
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
< Back
Next >
Cancel

Profile

Specify the profiles for which this rule applies.

When does this rule apply?

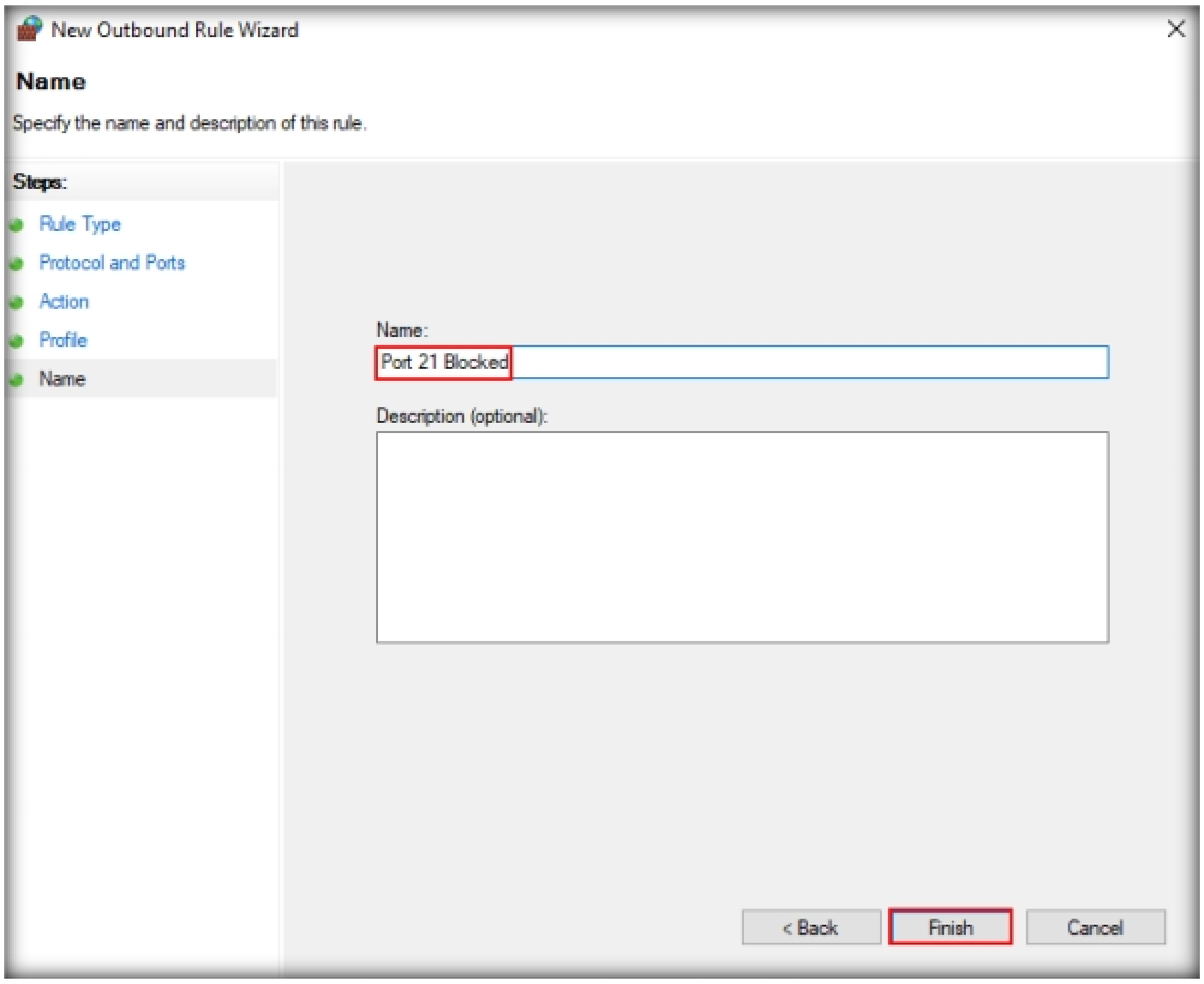
☑ **Domain**
Applies when a computer is connected to its corporate domain.

☑ **Private**
Applies when a computer is connected to a private network location, such as a home or work place.

☑ **Public**
Applies when a computer is connected to a public network location.

Figure 2.2.14: Windows Firewall Profile settings

26. In **Name**, type **Port 21 Blocked** in the **Name** field and click **Finish**.



New Outbound Rule Wizard
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
< Back
Finish
Cancel

Name

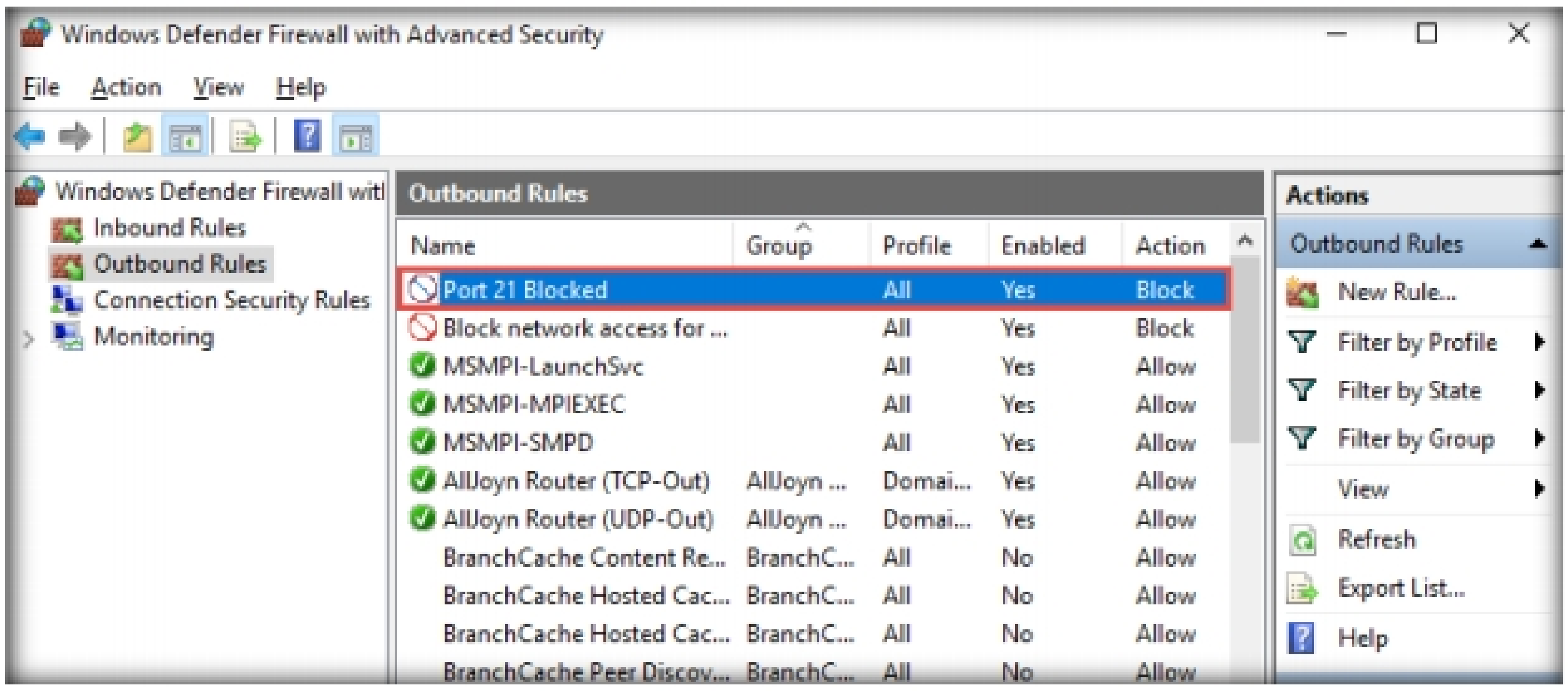
Specify the name and description of this rule.

Name: Port 21 Blocked

Description (optional):

Figure 2.2.15: Windows Firewall assigning a name to Port

27. The new rule **Port 21 Blocked** is created, as shown in the screenshot.



Windows Defender Firewall with Advanced Security
File
Action
View
Help
Windows Defender Firewall witl
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Actions
Outbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help

Outbound Rules

Name	Group	Profile	Enabled	Action
Port 21 Blocked		All	Yes	Block
Block network access for ...		All	Yes	Block
MSMPI-LaunchSvc		All	Yes	Allow
MSMPI-MPIEXEC		All	Yes	Allow
MSMPI-SMPD		All	Yes	Allow
AllJoyn Router (TCP-Out)	AllJoyn ...	Domai...	Yes	Allow
AllJoyn Router (UDP-Out)	AllJoyn ...	Domai...	Yes	Allow
BranchCache Content Re...	BranchC...	All	No	Allow
BranchCache Hosted Cac...	BranchC...	All	No	Allow
BranchCache Hosted Cac...	BranchC...	All	No	Allow
BranchCache Peer Discov...	BranchC...	All	No	Allow

Figure 2.2.16: Windows Firewall new rule

28. Right-click the newly created rule (**Port 21 Blocked**) and click **Properties**.

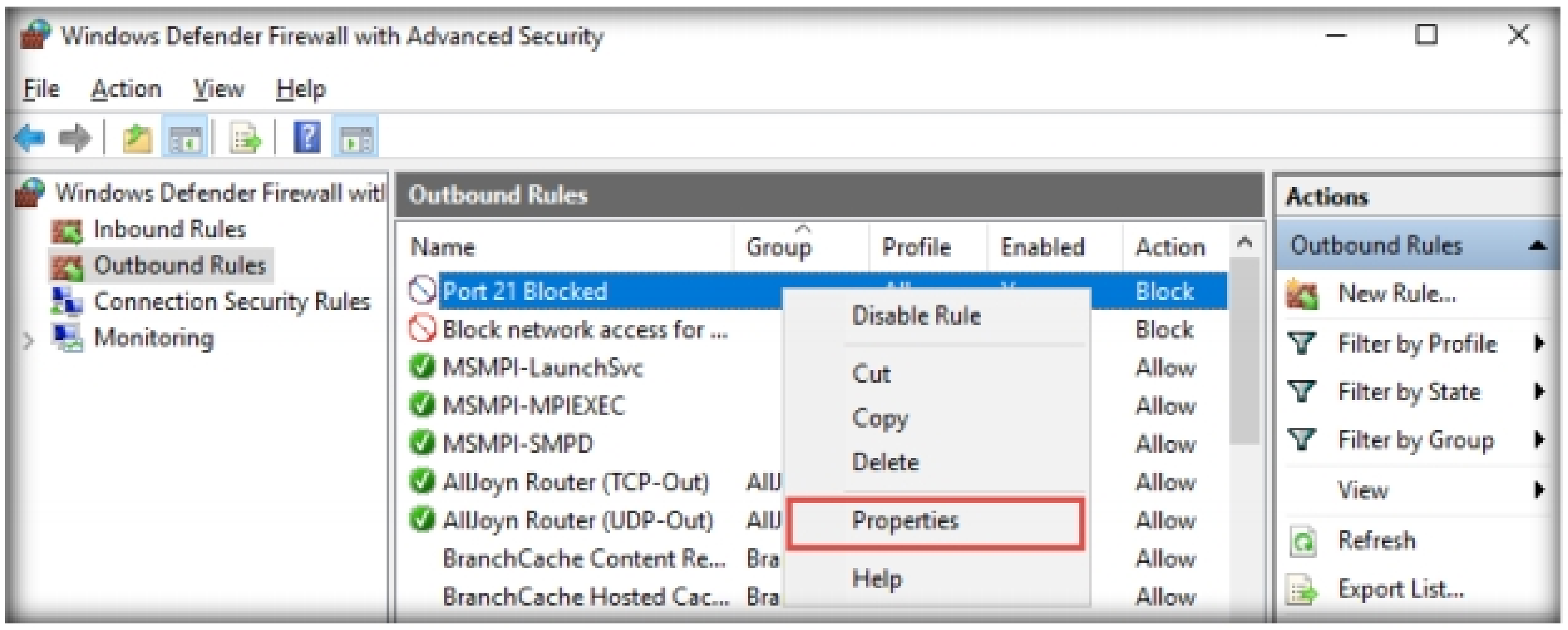
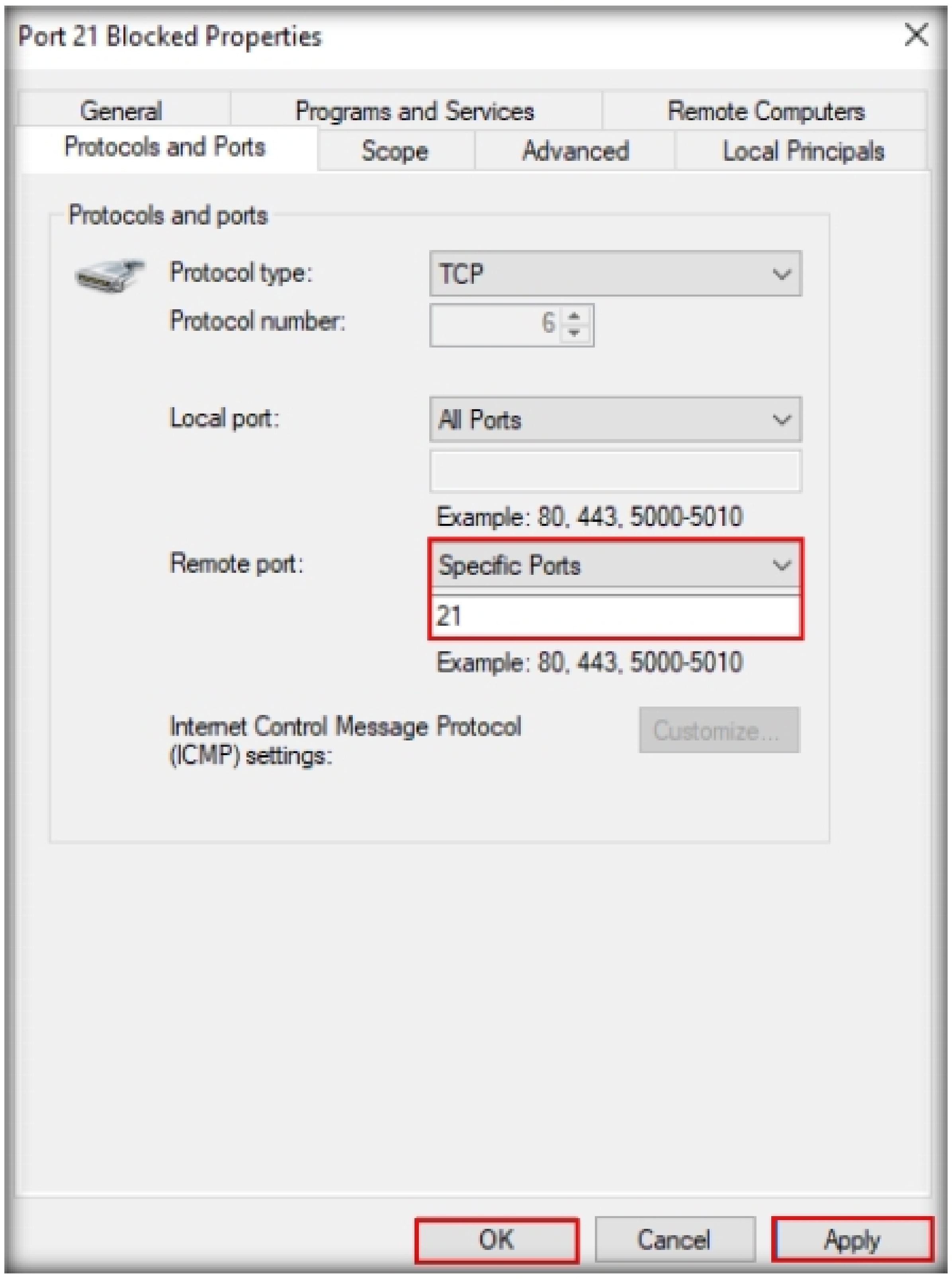

Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall witl
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Outbound Rules
Name Group Profile Enabled Action
Port 21 Blocked Block
Block network access for ... Block
MSMPI-LaunchSvc Allow
MSMPI-MPIEXEC Allow
MSMPI-SMPD Allow
AllJoyn Router (TCP-Out) AllJ Allow
AllJoyn Router (UDP-Out) AllJ Allow
BranchCache Content Re... Bra Allow
BranchCache Hosted Cac... Bra Allow
Disable Rule
Cut
Copy
Delete
Properties
Help
Actions
Outbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...

Figure 2.2.17: Windows Firewall new rule properties

29. The **Properties** window for **Port 21 Blocked** rule appears.

30. Select the **Protocols and Ports** tab. In the **Remote port**: field, select the **Specific Ports** option from the drop-down list and enter the port number as **21**.

31. Leave the other default settings, click **Apply**, and then click **OK**.


Port 21 Blocked Properties
General
Programs and Services
Remote Computers
Protocols and Ports
Scope
Advanced
Local Principals
Protocols and ports
Customize...
OK
Cancel
Apply

Protocol type: TCP
Protocol number: 6
Local port: All Ports
Example: 80, 443, 5000-5010
Remote port: Specific Ports
21
Example: 80, 443, 5000-5010
Internet Control Message Protocol (ICMP) settings:

Figure 2.2.18: Firewall Port 21 Blocked Properties

TASK 2.4

Test for Accessing FTP Site

32. Disable the rule and confirm that you can connect to the ftp site.

33. Right-click the newly added rule and click **Disable Rule**.

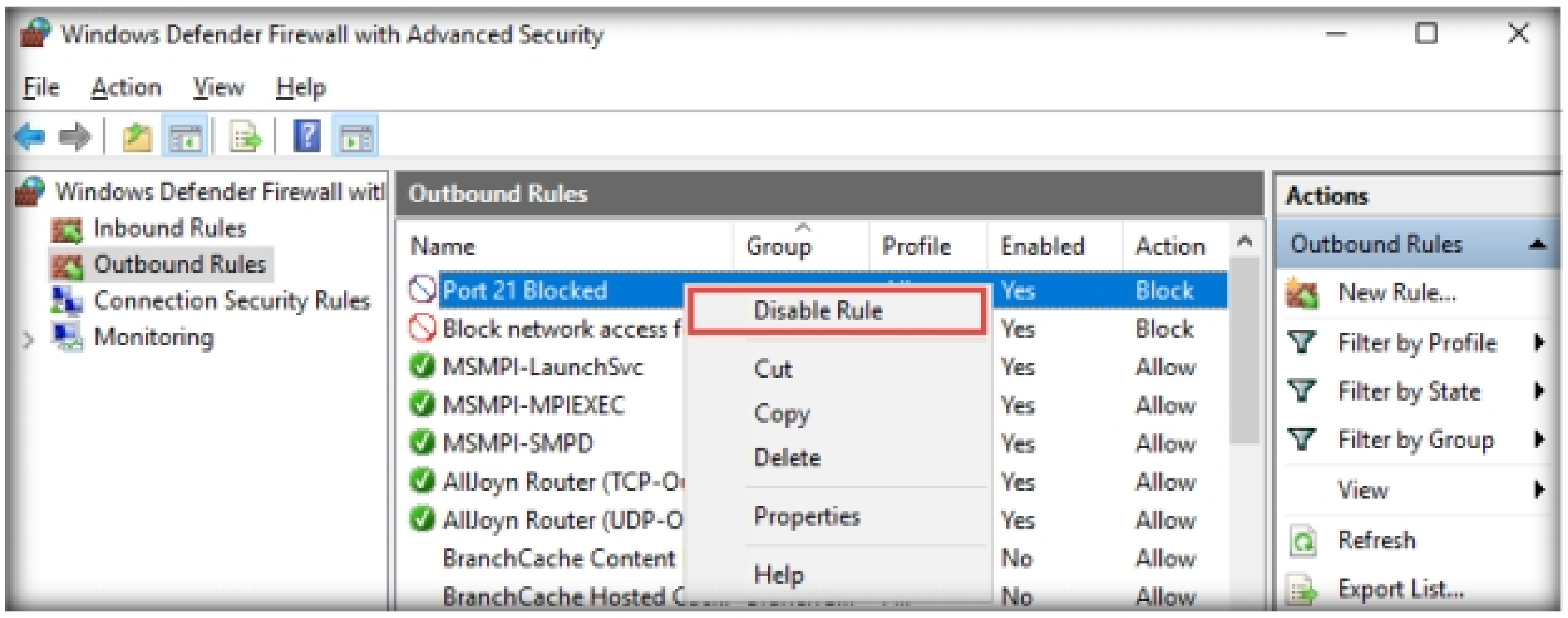
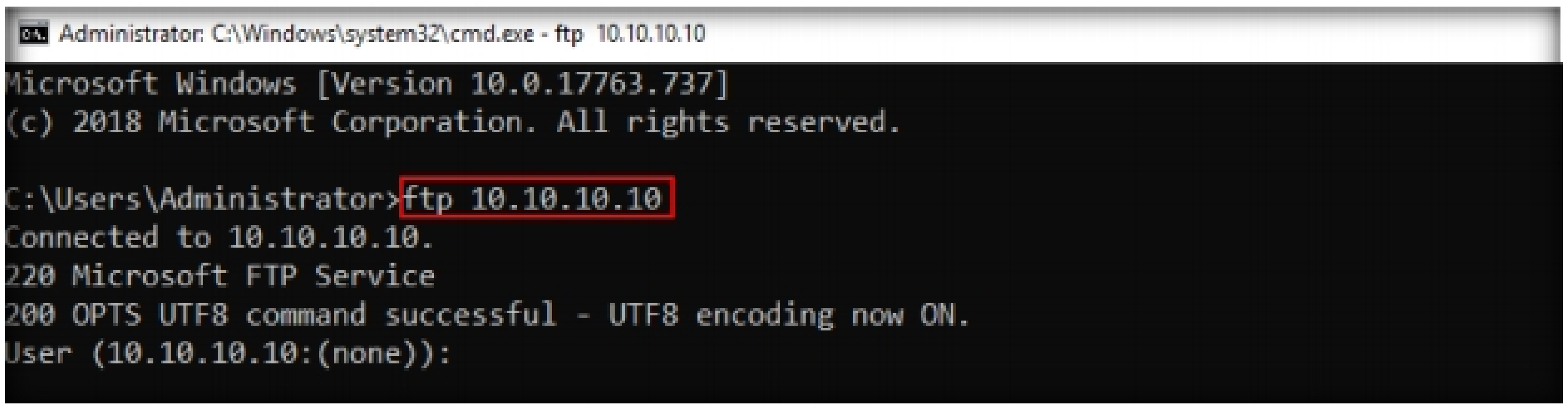

Windows Defender Firewall with Advanced Security
File
Action
View
Help
Windows Defender Firewall wit
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Outbound Rules
Name
Group
Profile
Enabled
Action
Port 21 Blocked
Block network access f
MSMPI-LaunchSvc
MSMPI-MPIEXEC
MSMPI-SMPD
AllJoyn Router (TCP-O
AllJoyn Router (UDP-O
BranchCache Content
BranchCache Hosted C
Yes
Block
Yes
Block
Yes
Allow
Yes
Allow
Yes
Allow
Yes
Allow
Yes
Allow
No
Allow
No
Allow
Disable Rule
Cut
Copy
Delete
Properties
Help
Actions
Outbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...

Figure 2.2.19: Disabling the outbound rule

34. Launch the command prompt and issue **ftp 10.10.10.10**. You will be asked to enter the username.


Administrator: C:\Windows\system32\cmd.exe - ftp 10.10.10.10

```
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ftp 10.10.10.10
Connected to 10.10.10.10.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (10.10.10.10:(none)):
```

Figure 2.2.20: Issuing FTP command

Note: In the above-mentioned command, **10.10.10.10** refers to the IP address of **Windows 10** where the ftp site is located. Make sure that you issue the IP address of Windows 10 in your lab environment.

35. This means you can establish an FTP connection, and then close the command prompt window.

36. Now, enable the rule and check whether you can establish a connection.

37. Right-click the newly added rule and click **Enable Rule**.

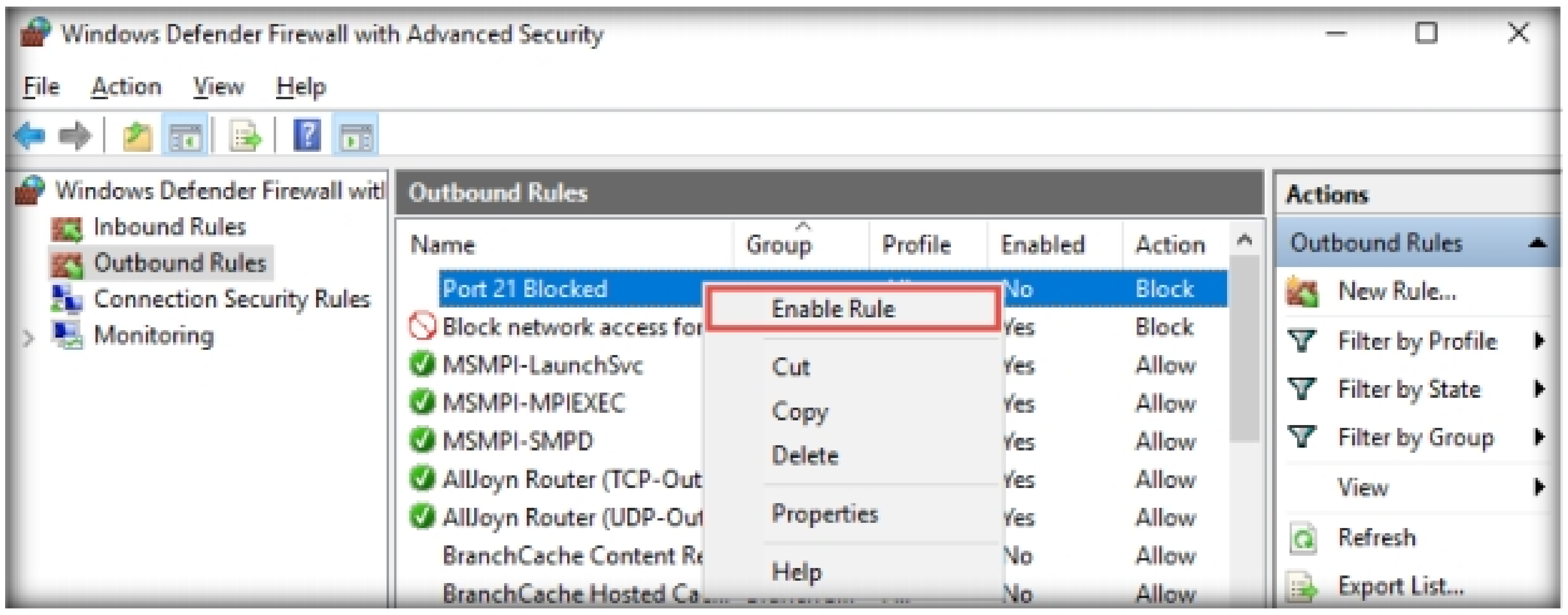
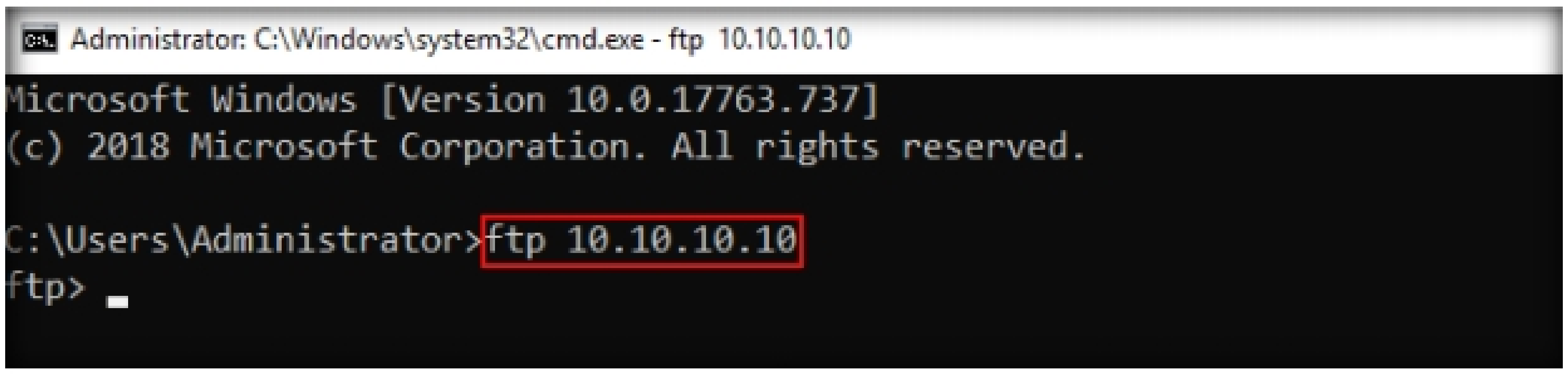

Windows Defender Firewall with Advanced Security
File
Action
View
Help
Windows Defender Firewall wit
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Outbound Rules
Name
Group
Profile
Enabled
Action
Port 21 Blocked
Block network access for
MSMPI-LaunchSvc
MSMPI-MPIEXEC
MSMPI-SMPD
AllJoyn Router (TCP-Out
AllJoyn Router (UDP-Out
BranchCache Content Re
BranchCache Hosted Ca
No
Block
Yes
Block
Yes
Allow
Yes
Allow
Yes
Allow
Yes
Allow
Yes
Allow
No
Allow
No
Allow
Enable Rule
Cut
Copy
Delete
Properties
Help
Actions
Outbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...

Figure 2.2.21: Enabling the outbound rule

38. Launch **Command Prompt** and check whether you can connect to the ftp site by issuing the command **ftp 10.10.10.10**.
39. The added outbound rule should block the connection, as shown in the screenshot.



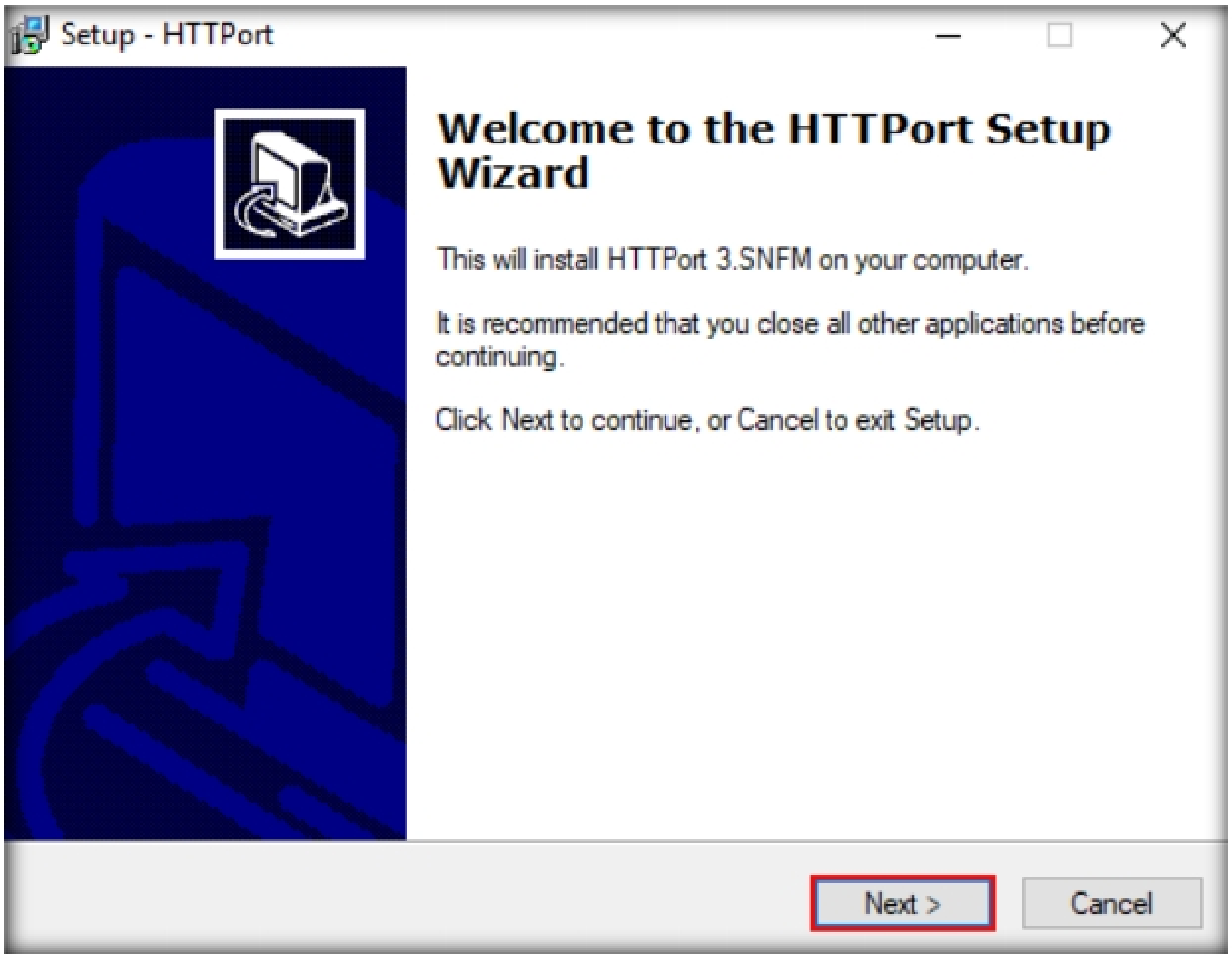
Administrator: C:\Windows\system32\cmd.exe - ftp 10.10.10.10

```
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ftp 10.10.10.10
ftp> _
```

Figure 2.2.22: Issuing FTP command

Note: In the above-mentioned command, **10.10.10.10** refers to the IP address of **Windows 10**, where the ftp site is located. Make sure that you issue the IP address of Windows 10 in your lab environment.

40. Now, we will perform **tunneling** using **HTTPort** to establish a connection with the FTP site located on **Windows 10**.
41. Navigate to **Z:\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots\HTTP Tunneling Tools\HTTPort** and double-click **httport3snfm.exe**.
42. If a **User Account Control** pop-up appears, click **Yes**.
43. Follow the installation steps to install HTTPort.



Welcome to the HTTPort Setup Wizard

This will install HTTPort 3.SNFM on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

Figure 2.2.23: HTTPort Setup wizard

TASK 2.5

Perform HTTP Tunneling

44. Launch HTTPort (**Httport3SNFM**) from the **Start** menu.

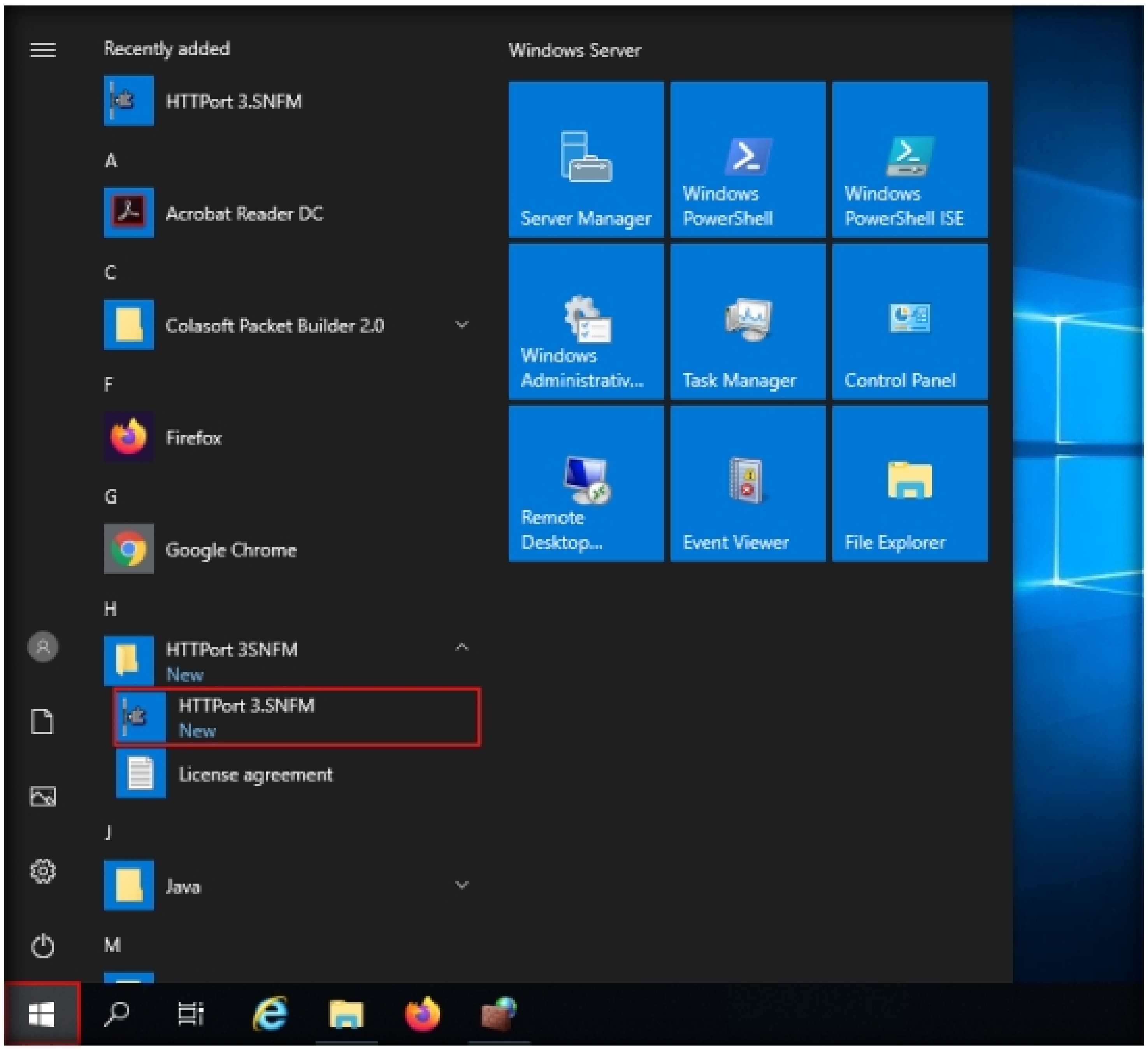
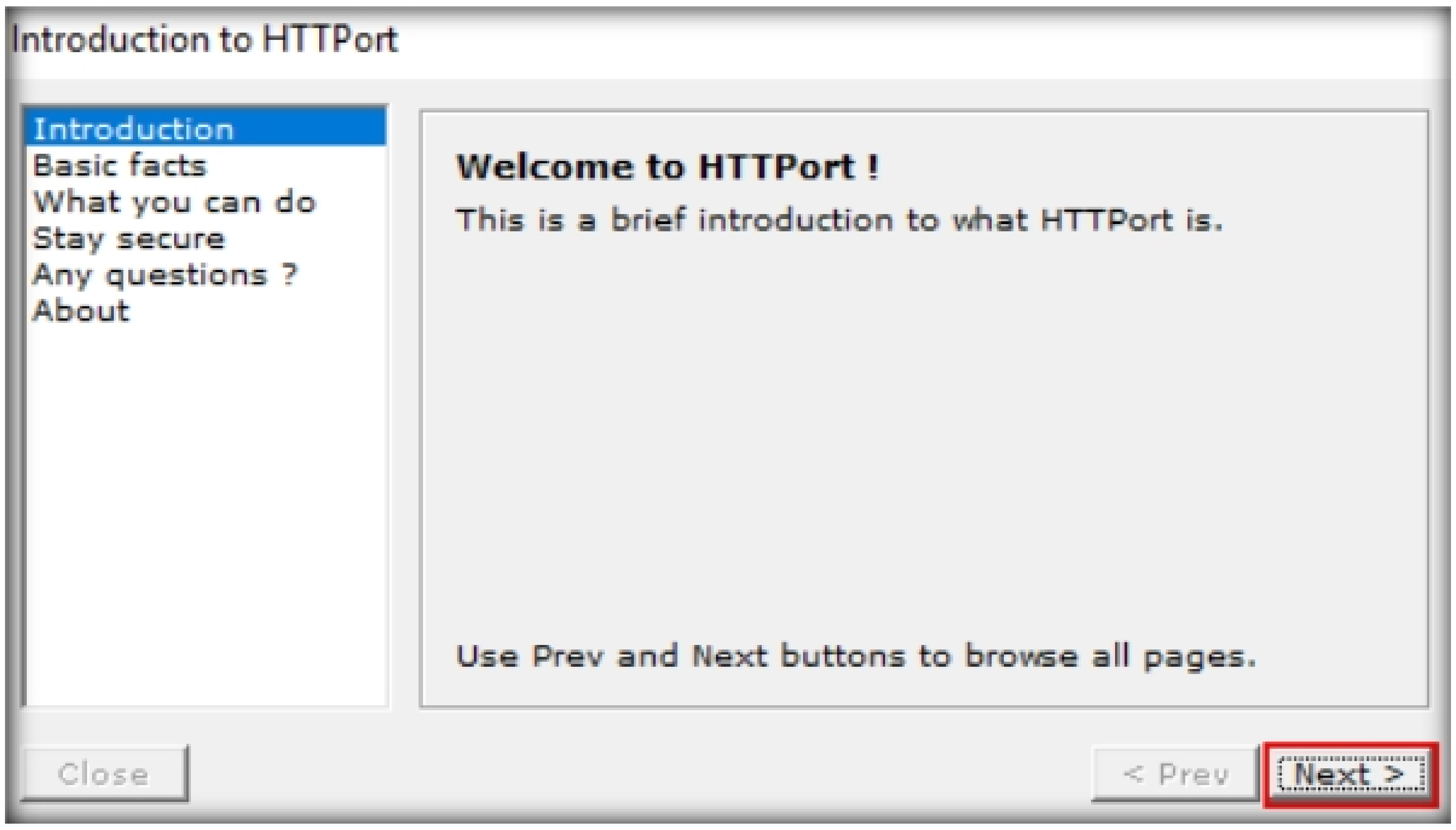

Recently added
HTTPort 3.SNFM
A
Acrobat Reader DC
C
Colasoft Packet Builder 2.0
F
Firefox
G
Google Chrome
H
HTTPort 3SNFM
New
HTTPort 3.SNFM
New
License agreement
J
Java
M
Windows Server
Server Manager
Windows PowerShell
Windows PowerShell ISE
Windows Administrativ...
Task Manager
Control Panel
Remote Desktop...
Event Viewer
File Explorer

Figure 2.2.24: Windows Server 2012 Apps screen

45. An **Introduction to HTTPort** wizard appears; click **Next** five times, until you come to the last wizard pane, and then click **Close**.


Introduction to HTTPort
Introduction
Basic facts
What you can do
Stay secure
Any questions ?
About
Close
< Prev
Next >

Welcome to HTTPort !

This is a brief introduction to what HTTPort is.

Use Prev and Next buttons to browse all pages.

Figure 2.2.25: Introduction to HTTPort wizard

46. The **HTTPort** main window (**HTTPort 3.SNFM**) appears, as shown in the screenshot.

47. On the **Proxy** tab, enter the **Host name** or **IP address** (**10.10.10.16**) of the machine where HTTHost is running (**Windows Server 2016**).

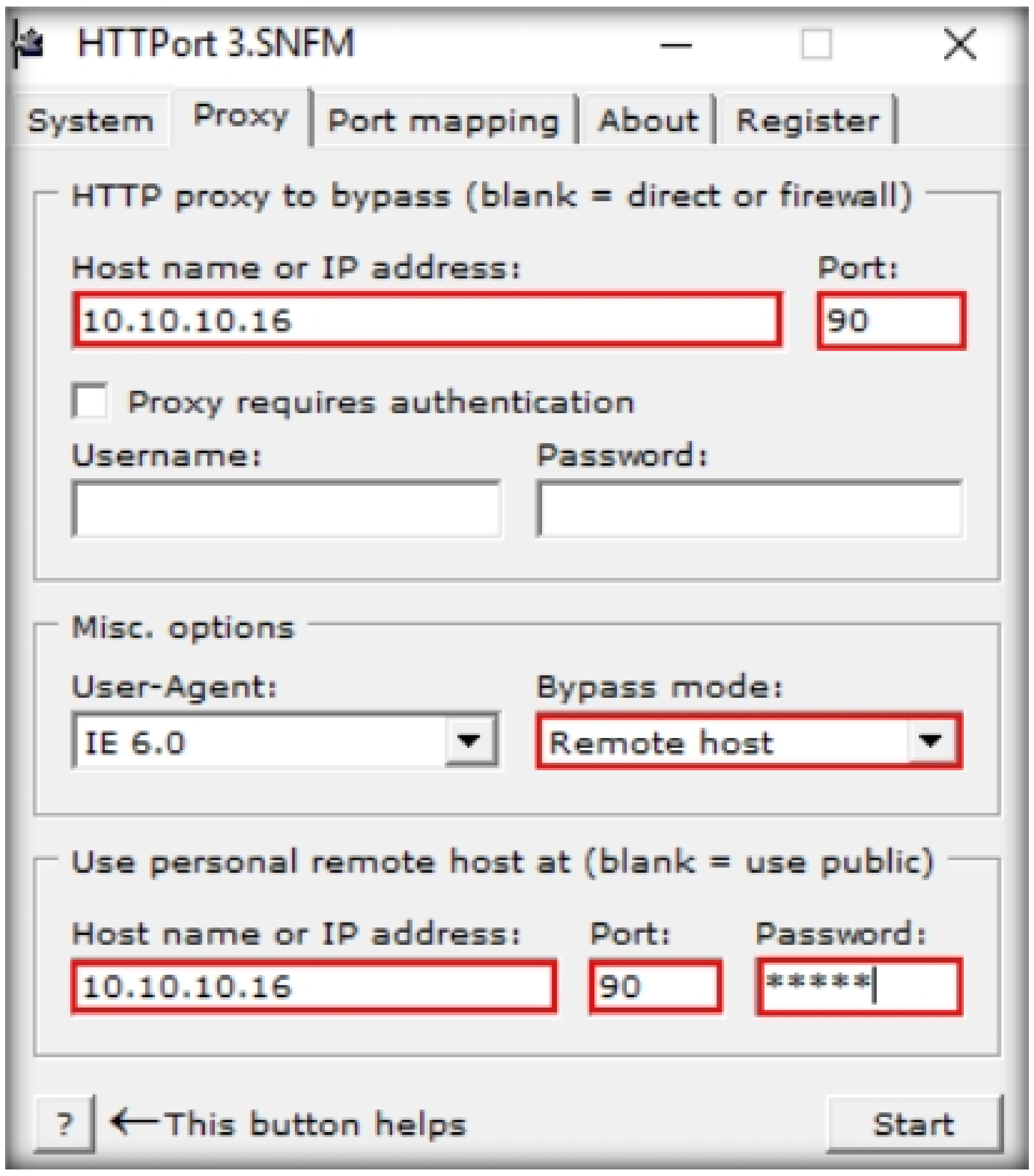
Note: The IP address of **Windows Server 2016** may vary in your lab environment.

48. Enter the **Port** number **90**.

49. In the **Misc. options** section, select **Remote host** from the **Bypass mode** drop-down list.

50. In the **Use personal remote host at (blank = use public)** section, re-enter the IP address of **Windows Server 2016** (**10.10.10.16**) and port number **90**.

51. Enter the password **magic** into the **Password** field.



HTTP proxy to bypass (blank = direct or firewall)

Host name or IP address: 10.10.10.16

Port: 90

☐ Proxy requires authentication

Username:

Password:

Misc. options

User-Agent: IE 6.0

Bypass mode: Remote host

Use personal remote host at (blank = use public)

Host name or IP address: 10.10.10.16

Port: 90

Password: *****

Figure 2.2.26: HTTPort Proxy settings window

52. Select the **Port mapping** tab, and click **Add** to create a new mapping.

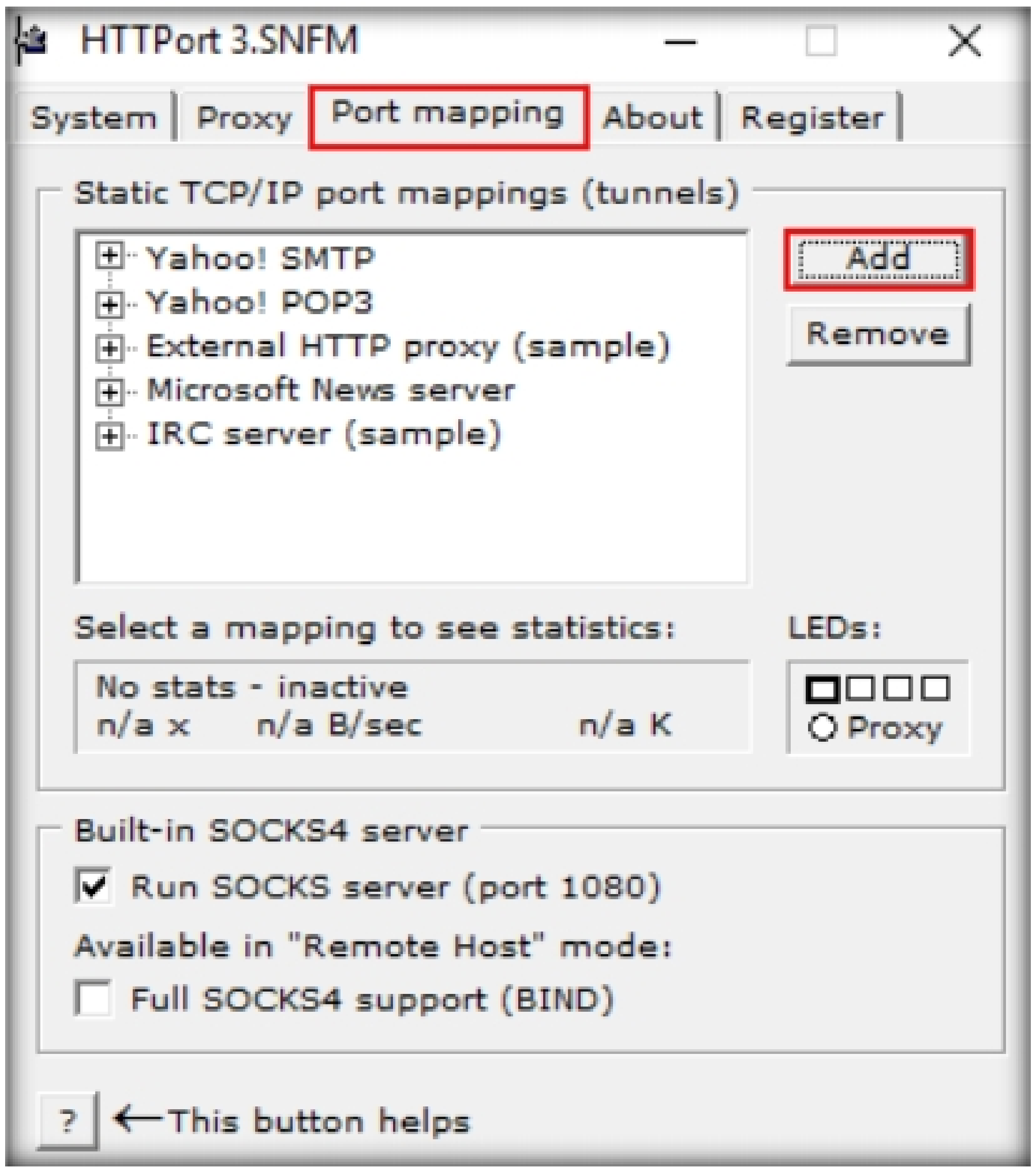

HTTPort 3.SNFM
System
Proxy
Port mapping
About
Register
Static TCP/IP port mappings (tunnels)
Yahoo! SMTP
Yahoo! POP3
External HTTP proxy (sample)
Microsoft News server
IRC server (sample)
Add
Remove
Select a mapping to see statistics:
LEDs:
No stats - inactive
n/a x n/a B/sec n/a K
○ Proxy
Built-in SOCKS4 server
☑ Run SOCKS server (port 1080)
Available in "Remote Host" mode:
☐ Full SOCKS4 support (BIND)
?
This button helps

Figure 2.2.27: HTTPort creating a new mapping

53. Right-click the **New mapping** node, and click **Edit**.

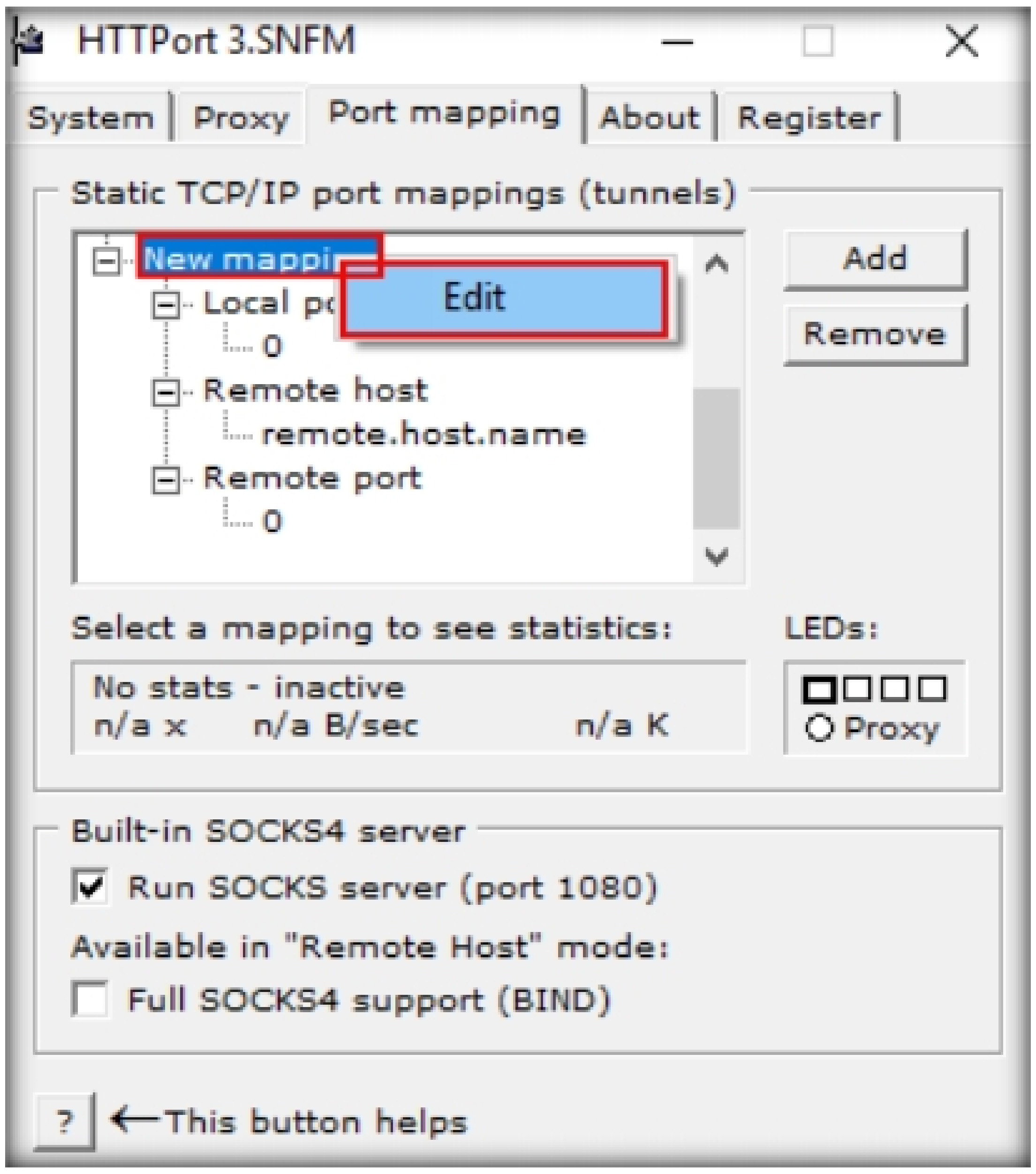
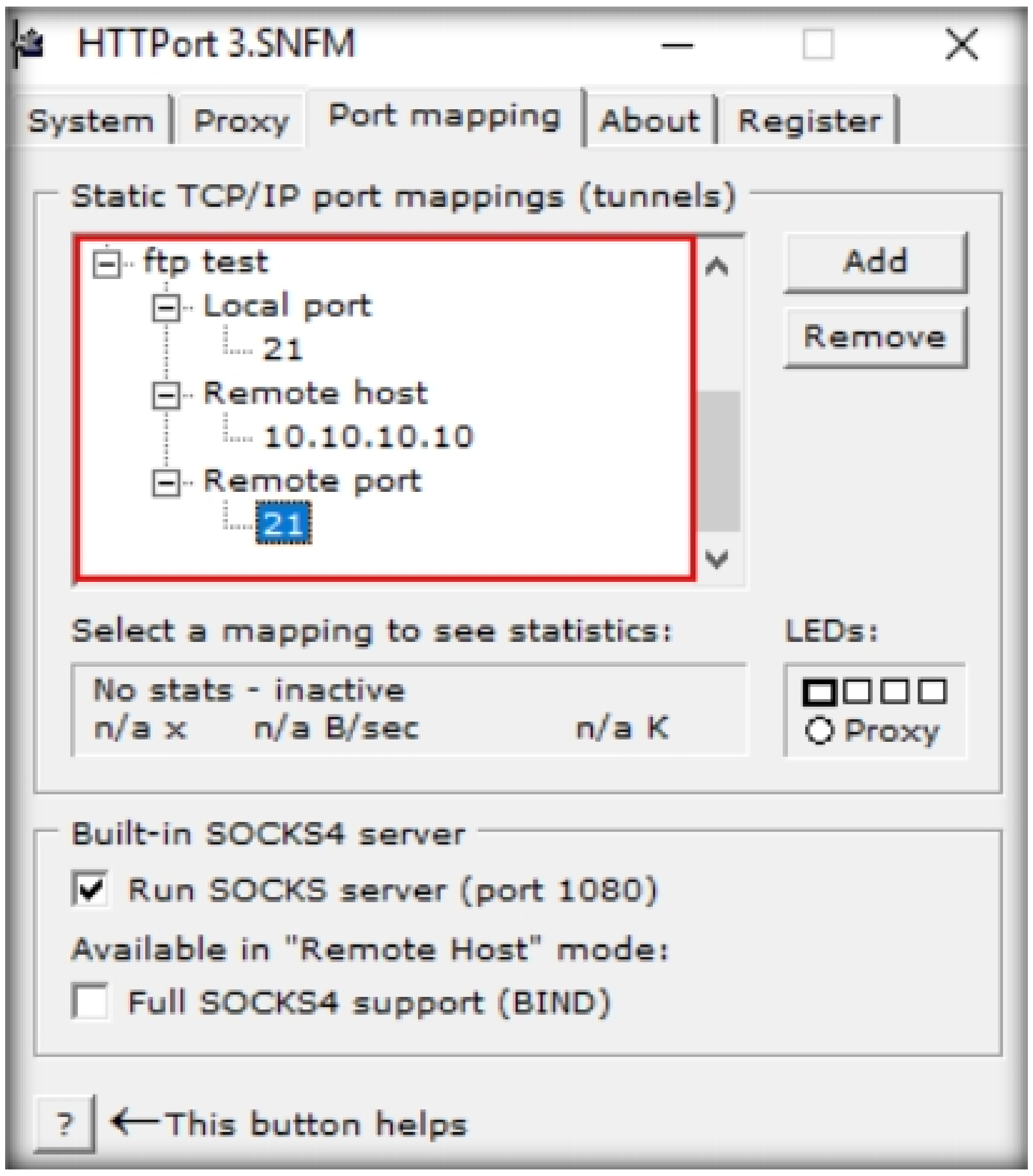

HTTPort 3.SNFM
System
Proxy
Port mapping
About
Register
Static TCP/IP port mappings (tunnels)
New mappi
Edit
Local pc
0
Remote host
remote.host.name
Remote port
0
Add
Remove
Select a mapping to see statistics:
LEDs:
No stats - inactive
n/a x n/a B/sec n/a K
○ Proxy
Built-in SOCKS4 server
☑ Run SOCKS server (port 1080)
Available in "Remote Host" mode:
☐ Full SOCKS4 support (BIND)
?
This button helps

Figure 2.2.28: HTTPort Editing to assign a mapping

54. Rename this as **ftp test** (you can enter the name of your choice).
55. Right-click the node below **Local port**; then click **Edit** and enter the port value as **21**.
56. Right-click the node below **Remote host**; click **Edit** and rename it as **10.10.10.10**.
57. Right-click the node below **Remote port**; then click **Edit** and enter the port value as **21**.

Note: **10.10.10.10** specifies in Remote host node is the IP address of the **Windows 10** machine that is hosting the FTP site.


HTTPort 3.SNFM
System
Proxy
Port mapping
About
Register
Add
Remove
LEDs:
Proxy
?
←This button helps

Static TCP/IP port mappings (tunnels)

```
ftp test
  Local port
    21
  Remote host
    10.10.10.10
  Remote port
    21
```

Select a mapping to see statistics:

No stats - inactive
n/a x   n/a B/sec   n/a K

Built-in SOCKS4 server

☑ Run SOCKS server (port 1080)

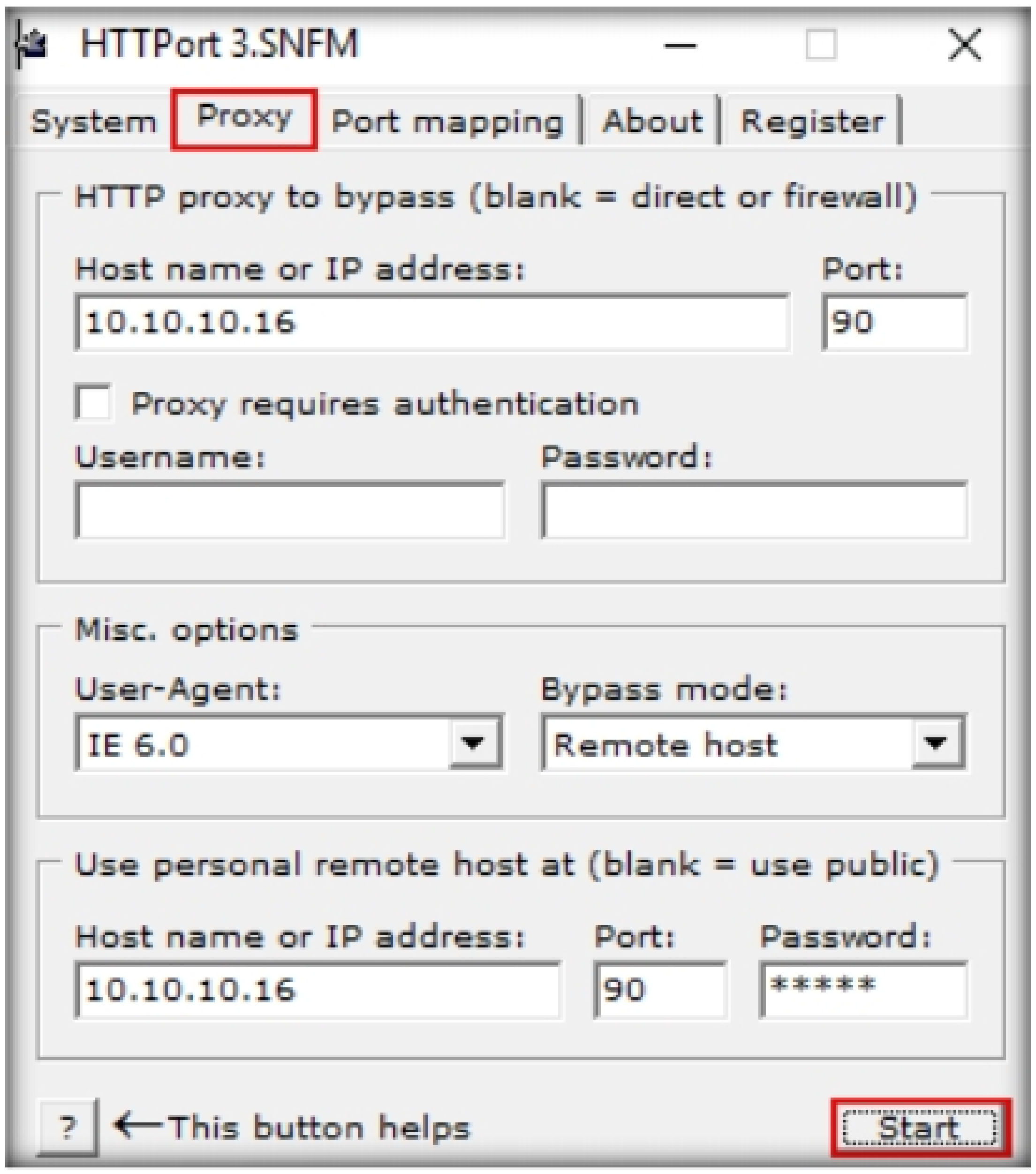
Available in "Remote Host" mode:

☐ Full SOCKS4 support (BIND)

Figure 2.2.29: HTTPort Static TCP/IP port mapping

58. Switch to the **Proxy** tab and click **Start** to begin the HTTP tunneling.

Note: If you get an error, ignore it.


HTTPort 3.SNFM
System
Proxy
Port mapping
About
Register
? ←This button helps
Start

HTTP proxy to bypass (blank = direct or firewall)
Host name or IP address: 10.10.10.16
Port: 90
☐ Proxy requires authentication
Username:
Password:

Misc. options
User-Agent: IE 6.0
Bypass mode: Remote host

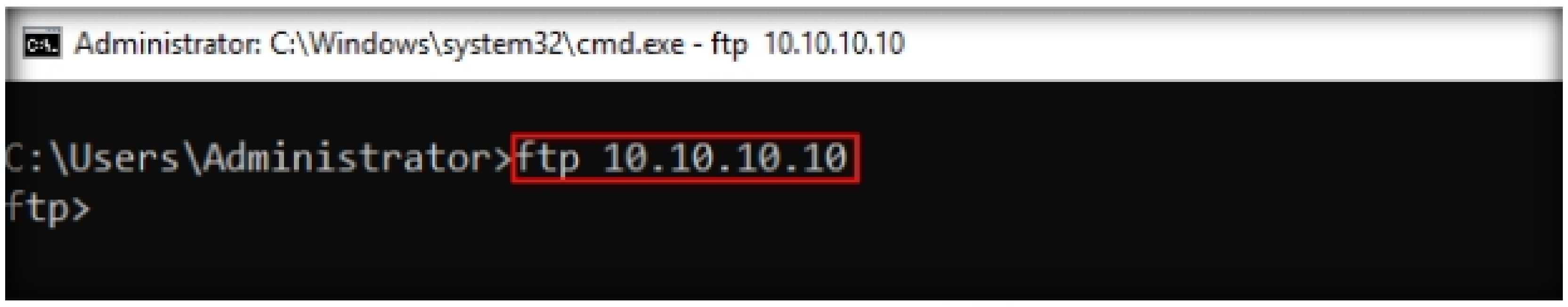
Use personal remote host at (blank = use public)
Host name or IP address: 10.10.10.16
Port: 90
Password: *****

Figure 2.2.30: HTTPort to start tunneling

59. HTTPort intercepts the ftp request to the localhost and tunnels through it. HTTHost is installed in the remote machine to connect you to **10.10.10.10**.

Note: This means you may not access the ftp site directly by issuing **ftp 10.10.10.10** in the command prompt, but you will be able to access it through the localhost by issuing the command **ftp 127.0.0.1**.

60. In **Windows Server 2019**; launch **Command Prompt**, type **ftp 10.10.10.10**, and press **Enter**. The ftp connection will be blocked by the outbound firewall rule.

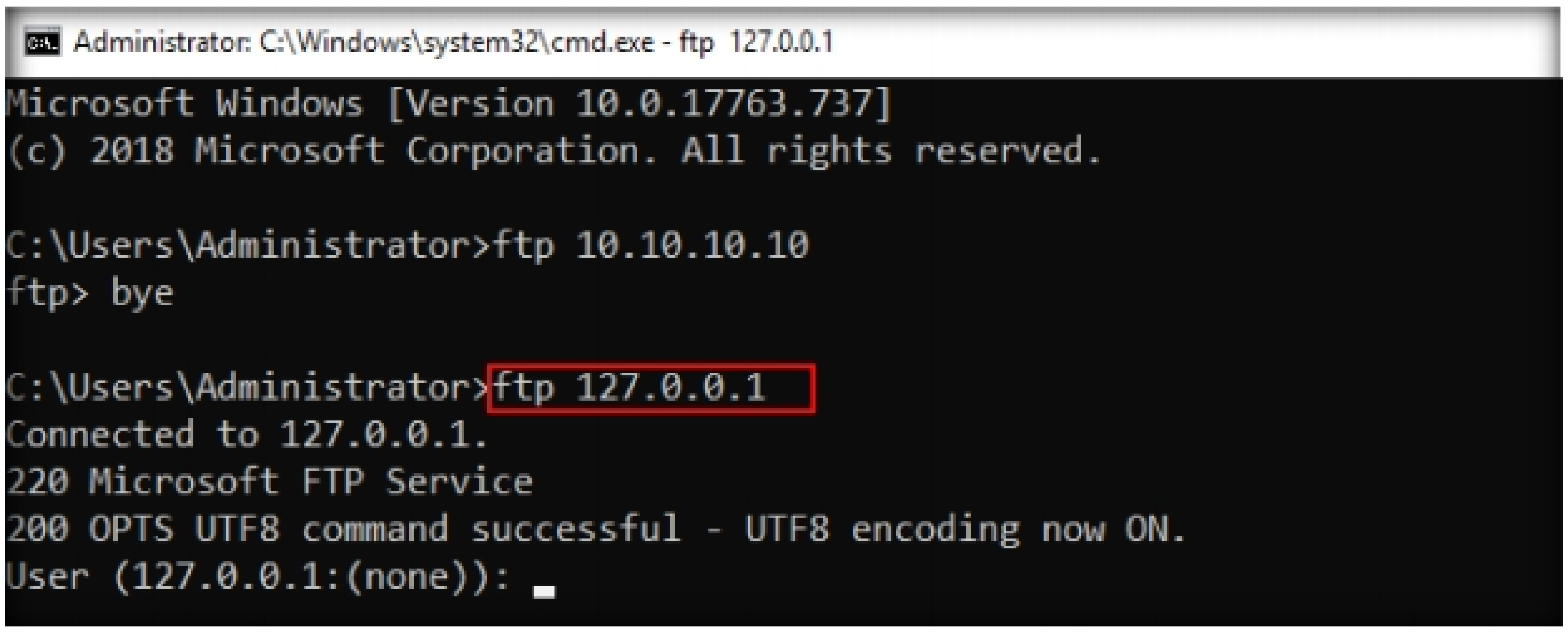

Administrator: C:\Windows\system32\cmd.exe - ftp 10.10.10.10

```
C:\Users\Administrator>ftp 10.10.10.10
ftp>
```

Figure 2.2.31: ftp connection is blocked

61. Now, launch a new **Command Prompt**, type **ftp 127.0.0.1**, and press **Enter**. You should be able to connect to the site.

Note: If you issue this command without starting HTTPort, the connection to the FTP site fails, stating that the FTP connection is refused.

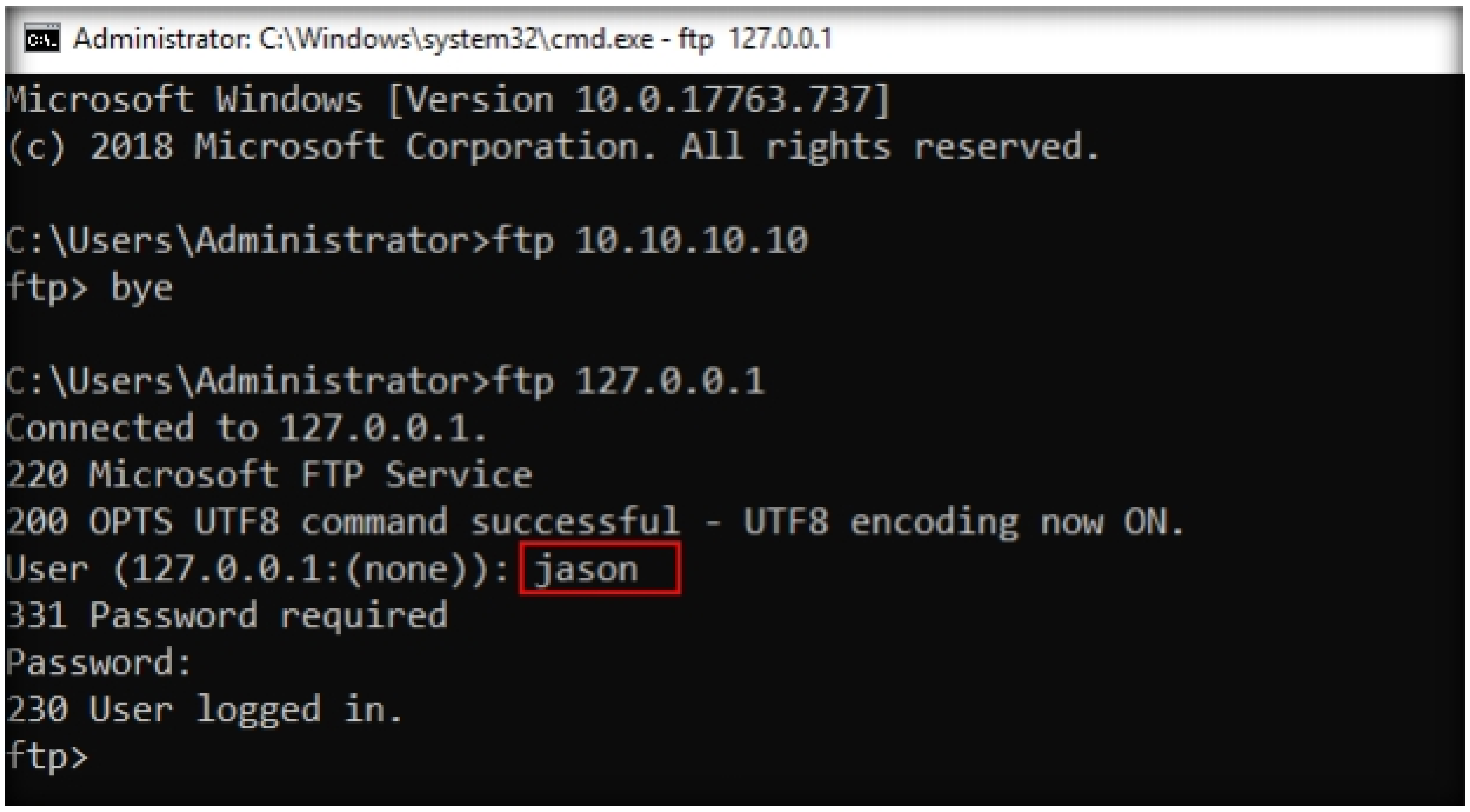


```
Administrator: C:\Windows\system32\cmd.exe - ftp  127.0.0.1
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ftp 10.10.10.10
ftp> bye

C:\Users\Administrator>ftp 127.0.0.1
Connected to 127.0.0.1.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (127.0.0.1:(none)): _
```

Figure 2.2.32: Executing ftp command

62. Enter the credentials of any user account on Windows 10. In this lab, we are using the credentials of the **Jason** account (username: **Jason**; Password: **qwerty**). Type the username and press **Enter**.

Note: The password you enter will not be visible.



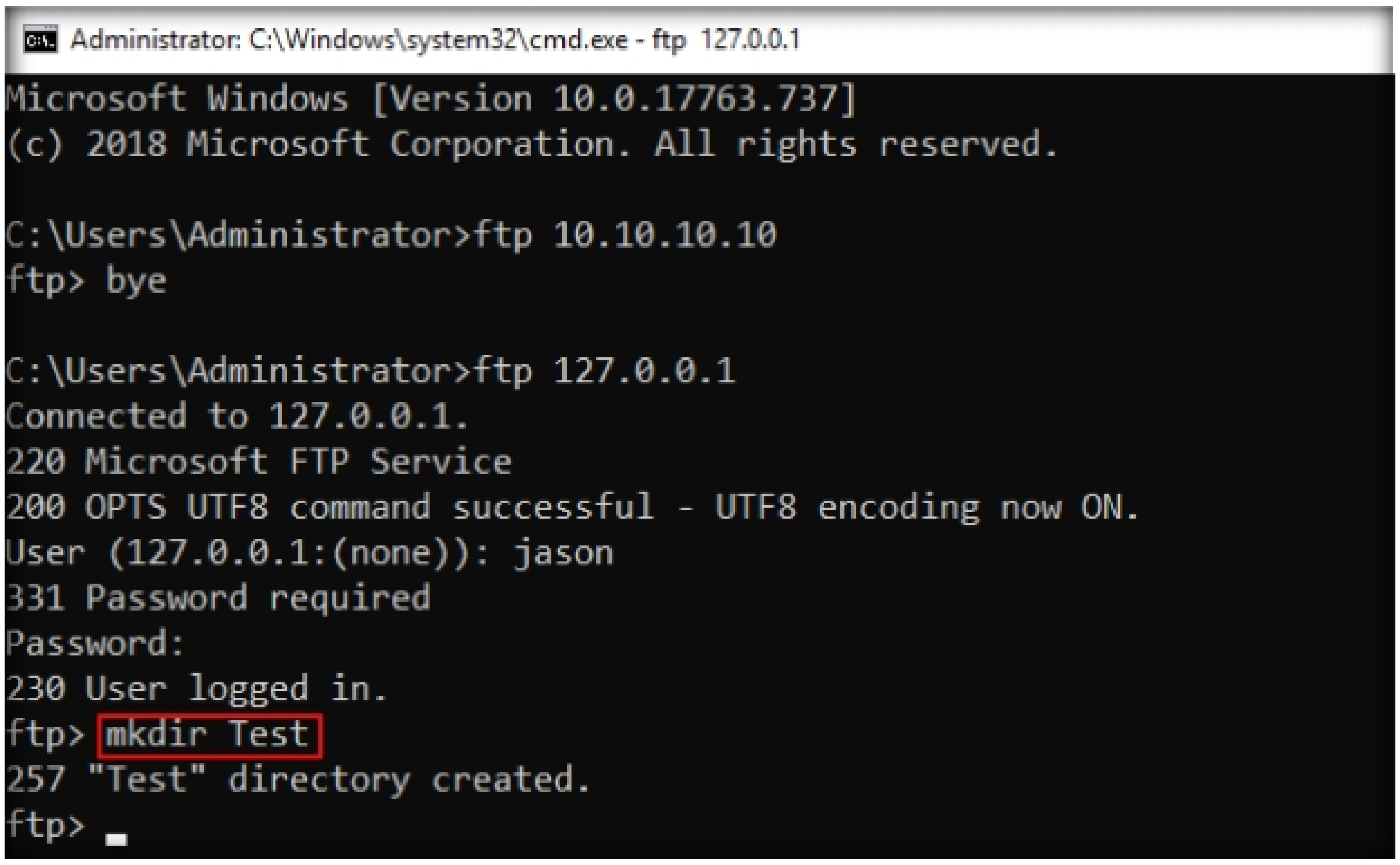
```
Administrator: C:\Windows\system32\cmd.exe - ftp  127.0.0.1
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ftp 10.10.10.10
ftp> bye

C:\Users\Administrator>ftp 127.0.0.1
Connected to 127.0.0.1.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (127.0.0.1:(none)): jason
331 Password required
Password:
230 User logged in.
ftp>
```

Figure 2.2.33: Signing in to the FTP site

63. You are successfully logged in, even after adding a firewall outbound rule inferring that a tunnel has been established by HTTPort and HTTHost and therefore have bypassed the firewall.

64. Now you have the access and ability to add files in the ftp directory located in the **Windows 10** virtual machine.

65. Type **mkdir Test** and press **Enter**.



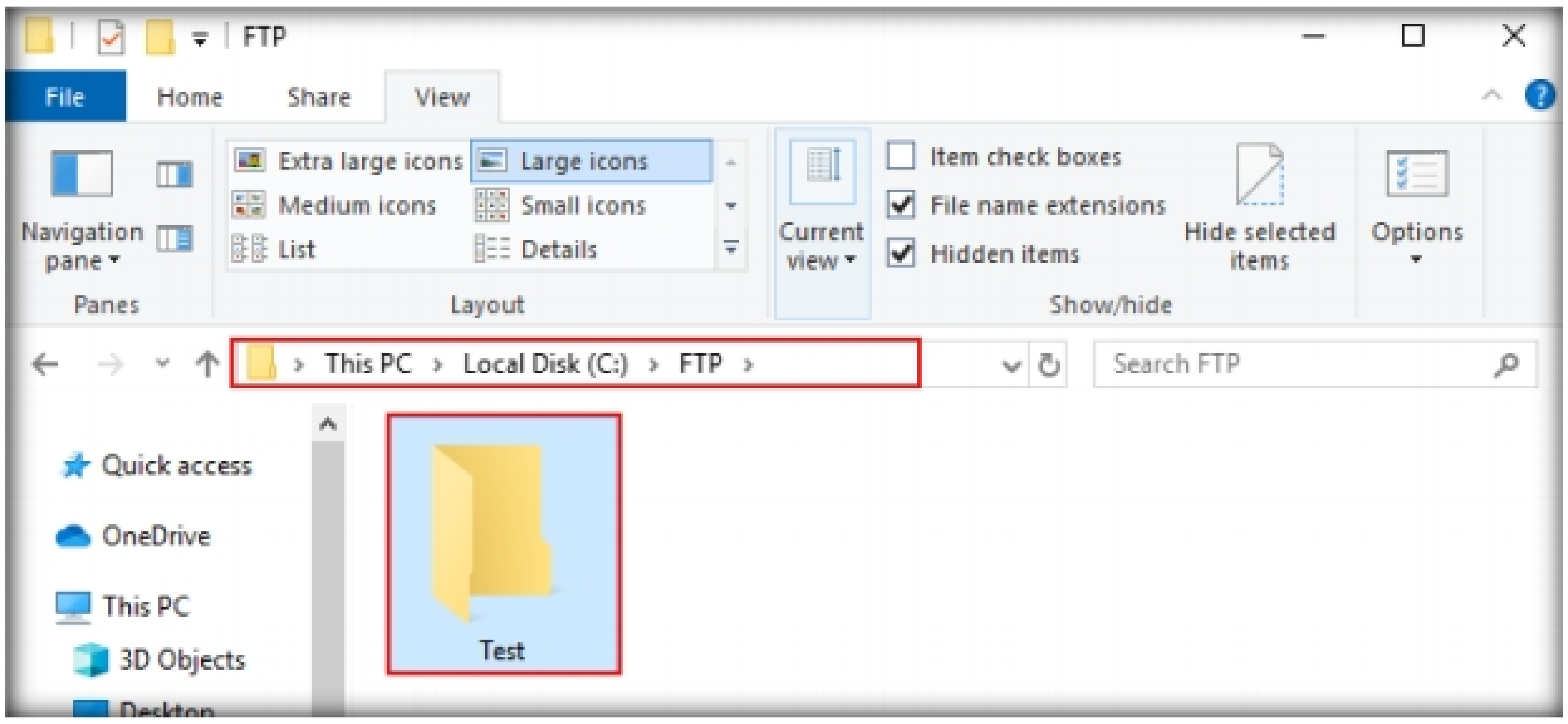
Administrator: C:\Windows\system32\cmd.exe - ftp 127.0.0.1

```
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ftp 10.10.10.10
ftp> bye

C:\Users\Administrator>ftp 127.0.0.1
Connected to 127.0.0.1.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (127.0.0.1:(none)): jason
331 Password required
Password:
230 User logged in.
ftp> mkdir Test
257 "Test" directory created.
ftp> _
```

Figure 2.2.34: Creating a directory

66. Now, switch to the **Windows 10** machine.

67. A directory named **Test** will be created in the **FTP** folder on the **Windows 10** (location: **C:\FTP**) virtual machine, as shown in the screenshot:



FTP
File
Home
Share
View
Navigation pane
Panes
Extra large icons
Large icons
Medium icons
Small icons
List
Details
Layout
Current view
☐ Item check boxes
☑ File name extensions
☑ Hidden items
Hide selected items
Show/hide
Options
This PC > Local Disk (C:) > FTP >
Search FTP
Quick access
OneDrive
This PC
3D Objects
Desktop
Test

Figure 2.2.35: New directory created

68. Thus, you are able to bypass HTTP proxies as well as firewalls, and thereby access files beyond them.

Note: On completion of the lab, delete the created outbound rule, stop HTTHost and HTTPort and disable the firewall (which was enabled in the beginning of the lab) in the machine (i.e., **Windows Server 2019**), and start the World Wide Web Publishing and IIS Admin Services on the **Windows Server 2016** virtual machine.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs